

**16<sup>th</sup> International Command and Control  
Research and Technology Symposium**  
**“Collective C2 in Multinational Civil-Military Operations”**

**Applicability of Visual Analytics to  
Defence and Security Operations**

***Primary Topic:***

Primary Topic: 4 - Information and Knowledge Exploitation

***Alternate Topics:***

Alternate Topic: 8 - Architectures, Technologies, and Tools

Alternate Topic: 10 - C2, Management, and Governance in Civil-Military Operations

***Authors:***

**Valérie Lavigne, Denis Gouin**

Innovative Interfaces and Interactions Group

Defence R&D Canada – Valcartier

2459 Pie-XI North, Quebec City, QC, G3J 1X5

Canada

***Point of Contact :***

**Valérie Lavigne**

E-mail: [valerie.lavigne@drdc-rddc.gc.ca](mailto:valerie.lavigne@drdc-rddc.gc.ca)

Phone: 1 (418) 844-4000 ext. 4114

Fax: 1 (418) 844-4538

<b>Report Documentation Page</b>			<i>Form Approved OMB No. 0704-0188</i>	
<p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>				
1. REPORT DATE <b>JUN 2011</b>	2. REPORT TYPE	3. DATES COVERED <b>00-00-2011 to 00-00-2011</b>		
4. TITLE AND SUBTITLE <b>Applicability of Visual Analytics to Defence and Security Operations</b>			5a. CONTRACT NUMBER	
			5b. GRANT NUMBER	
			5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)			5d. PROJECT NUMBER	
			5e. TASK NUMBER	
			5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Defence R&amp;D Canada ? Valcartier, Innovative Interfaces and Interactions Group, 2459 Pie-XI North, Quebec (Quebec), Canada, G3J 1X5,</b>			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)	
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>				
13. SUPPLEMENTARY NOTES <b>Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.</b>				
14. ABSTRACT <b>In the context of modern defence and security operations, analysts are faced with a continuously growing set of information of different nature which causes significant information overload problems and prevent developing good situation awareness. Fortunately, Visual Analytics (VA) has emerged as an efficient way of handling and making sense of massive data sets by exploiting interactive visualization technologies and human cognitive abilities. Defence R&amp;D Canada has conducted a review of the applicability of VA to support military and security operations. This paper is meant to provide someone new to this area with a quick overview of the current state of the art in visual analytics. First, we introduce the important scientific visualization, interaction and reasoning concepts supporting VA. Then, we present some visual analytics advanced techniques. The VA requirements are described for four application domains: maritime domain awareness, military intelligence analysis, cyber security and emergency management, along with promising research projects and commercial software. Finally, we identify key organizations and initiatives in this research field and relevant resources.</b>				
15. SUBJECT TERMS				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>50</b>
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>	19a. NAME OF RESPONSIBLE PERSON	

# Applicability of Visual Analytics to Defence and Security Operations

**Valérie Lavigne**

Defence R&D Canada – Valcartier  
2459 Pie-XI Blvd. North  
Quebec (Quebec), Canada, G3J 1X5  
valerie.lavigne@drdc-rddc.gc.ca

**Denis Gouin**

Defence R&D Canada – Valcartier  
2459 Pie-XI Blvd. North  
Quebec (Quebec), Canada, G3J 1X5  
denis.gouin@drdc-rddc.gc.ca rdc-rddc.gc.ca

## Abstract

In the context of modern defence and security operations, analysts are faced with a continuously growing set of information of different nature which causes significant information overload problems and prevent developing good situation awareness. Fortunately, Visual Analytics (VA) has emerged as an efficient way of handling and making sense of massive data sets by exploiting interactive visualization technologies and human cognitive abilities. Defence R&D Canada has conducted a review of the applicability of VA to support military and security operations. This paper is meant to provide someone new to this area with a quick overview of the current state of the art in visual analytics. First, we introduce the important scientific visualization, interaction and reasoning concepts supporting VA. Then, we present some visual analytics advanced techniques. The VA requirements are described for four application domains: maritime domain awareness, military intelligence analysis, cyber security and emergency management, along with promising research projects and commercial software. Finally, we identify key organizations and initiatives in this research field and relevant resources.

## 1 Introduction

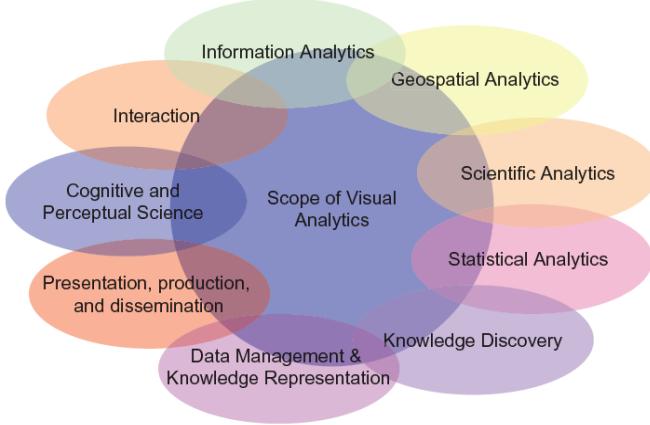
In the era of the information age, decision makers and first responders in Defence and Security are faced with increasing amounts of dynamic information originating from a wide variety of sources and in a wide variety of formats, which they need to analyse in order to understand a situation and react promptly. This is the case for example, in situation management following a natural or man-made disaster, a terrorist attack, a military conflict, a pandemic flu or a criminal series of activities. In developing Situation Awareness (SA), analysts must understand how a situation has developed and how it may develop. They need to identify trends and patterns. They need to work in collaboration with representatives from different organizations.

Although information fusion and rule-based systems have shown their value in helping making sense of information and providing situation awareness, during the last decade, a new science and technology called Visual Analytics (VA) has rapidly emerged in helping users understand a situation by cleverly representing the information and providing mechanisms to interact with the information.

This paper is meant to provide someone new to this area with a quick overview of the current state of the art in visual analytics. We begin with an introduction of the important scientific visualization, interaction and reasoning concepts supporting VA and we present some visual analytics advanced techniques. Then the VA requirements are described for four application domains: maritime domain awareness, military intelligence analysis, cyber security and emergency management, along with promising research projects and commercial software. Finally, we identify key organizations and initiatives in this research field and relevant resources.

## 2 Visual Analytics

“Visual analytics is the science of analytical reasoning facilitated by interactive visual interfaces.” This is the most widespread definition of VA and it comes from the US research agenda that launched the field: *Illuminating the Path* (Thomas and Cook, 2005).

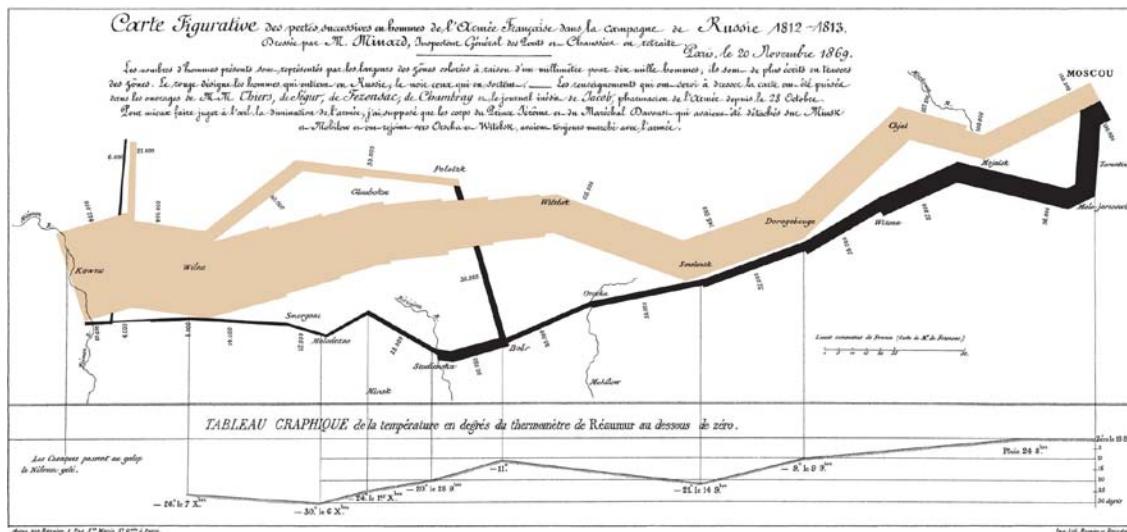


**Figure 1: Visual analytics as a highly interdisciplinary field of research (Thomas, 2009).**

VA is a multidisciplinary field that combines various related research areas where much valuable prior work has been done. Figure 1 shows a non-exhaustive list of scientific disciplines that are related to VA (Thomas, 2009). The challenge of making visual analysis effective calls for advancement in a variety of scientific fields. Visualization, interaction science and analytical reasoning are three research domains that bring highly important scientific concepts to VA and these are described in the following sections.

## 2.1 Visualization

Humans discovered a long time ago that they could enhance their cognitive abilities by using external representation aids (Card et al., 1999). The use of visualization to present information is not a new phenomenon. It has been used in maps, scientific drawings and data plots for over a thousand years. For example, Figure 2 shows Minard's map of Napoleon's invasion of Russia. This flow map was published in 1869 on the subject of Napoleon's disastrous Russian campaign of 1812.



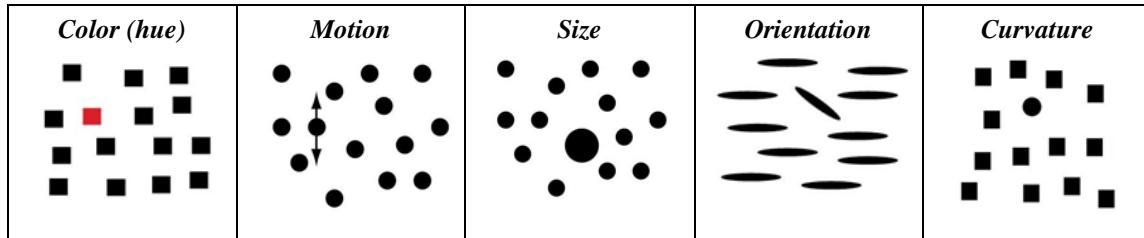
*Figure 2: Representation of Napoleon's invasion of Russia (Minard, 1869).*

The graph displays several variables in a single two-dimensional image:

- the army's location and direction, showing where units split off and rejoined,
- the declining size of the army (note e.g. the crossing of the Berezina river on the retreat),
- and the low temperatures during the retreat.

The intent of visualization is not merely to display information using pictures. The visual representation should be designed in a meaningful way in order to provide insight to the user. The optimal choice is highly dependent on the data involved and the task to be performed.

Information can be presented visually using points, lines, shapes, colors, intensity, textures, motion, etc. To select effective visual cues for data representation, we can use results obtained from the study of human perception. Preattentive features form a set of visual properties that are detected very rapidly and accurately by the low-level visual system. These properties were initially called preattentive since their detection seems to precede focused attention. This process is effortless, meaning that it does not demand attentional resources for a human. In each case presented in Figure 3, a unique visual property in the target allows it to “pop out” of the display. Examples of tasks that can be performed using preattentive features are: target detection, boundary detection, region tacking; and counting and estimation (Healey, 2009). In Figure 4, the use of semantic depth of field makes some chess pieces more salient to guide user’s attention (Kosara et al., 2001).



*Figure 3: Examples of preattentive visual features (adapted from Healey, 2009).*



*Figure 4: Semantic depth of field relies on preattentive features to offer a focus + context view. Focusing effects can highlight information (Kosara et al., 2001).*

Color in information presentation is mostly used to distinguish one element from another (Stone, 2006). Contrasting colors are different and draws attention, while analogous colors are similar and groups elements (see Figure 5). As Tufte (1990) puts it: “avoiding catastrophe becomes the first principle in bringing color to information: Above all, do no harm.” Chosen poorly, colors can obscure the meaning of information.

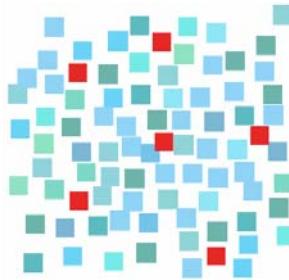


Figure 5: Contrast and analogy (Stone, 2006).

The Gestalt laws of organization describe how people perceive visual components as organized patterns or wholes, instead of many different parts (Koffka, 1935; Wertheimer, 1938). According to this theory, there are six main factors that determine how we group things according to visual perception: closure, similarity, proximity, symmetry, continuity and common fate.

Inattentional blindness, also known as perceptual blindness, refers to the inability to perceive features in a visual scene when the observer is not expecting them. Salient features within the visual field will not be observed if not processed by attention because the amount of information processed at any particular time is limited. In an experiment, 50% of subjects that were asked to watch a short video in which two groups of people pass a basket ball around and asked to count the number of passes failed to notice that a woman wearing a gorilla suit had walked through the scene (Simons and Chabris, 1999).

## 2.2 Interaction

Interaction enables the user to explore the data, try out hypotheses, drill into data, gain insight and collect knowledge. Human computer interaction has been an active research field for many years and is the study of interaction between people and computers. Visualization is considered interactive if control of some aspect of the information presented is available through a human input and the changes made by the user are incorporated in a timely manner.

Three categories of responsiveness (0.1s, 1s, and 10s) have been suggested to give an order of magnitude of the required response time for interactivity (Miller, 1968; Card, Robertson and Mackinlay, 1991). 0.1s is the upper limit for the system response to feel instantaneous. After more than 1s, the user's flow of thought is interrupted and the user loses the feeling of operating directly on the data. For delays longer than 10s, users will want to perform other tasks while waiting for the computer calculation to complete.

The famous visual information seeking mantra for designing advanced graphical user interfaces “overview first, zoom/filter, details on demand” comes from the interaction taxonomy from Shneiderman (1996). More recently, Soo Yi et al. (2007) proposed seven general categories of interaction techniques in information visualization:

- *Select*: mark something as interesting;
- *Explore*: show me something else;
- *Reconfigure*: show me a different arrangement;
- *Encode*: show me a different representation;
- *Abstract/Elaborate*: show me more or less detail;
- *Filter*: show me something conditionally;
- *Connect*: show me related items.

These categories are organized around the user's intent while interacting with the system rather than the low-level interaction techniques provided by the system. Soo Yi et al. (2007) also point out that "for different representation techniques, different interaction techniques are used to perform a similar task or achieve a similar goal".

### 2.3 Analytical Reasoning

Visual analytics is intended to be an active, engaging exploratory process of discovery. This human-information discourse is between the analyst and his data. It supports three goals: assessment (understand current situation and explain past events), forecasting (estimate future capabilities, threats, vulnerabilities and opportunities) and planning (develop options, create possible scenarios, prepare reactions to potential events). Analysts apply reasoning techniques in order to achieve these goals. Visual analytics is meant to facilitate high quality analysis with a limited quantity of user's time. Six basic ways were identified in how information visualization can expand human cognition (Card et al., 1999; Ware, 2000).

- Increased resources: high-bandwidth hierarchical interaction, parallel conceptual processing, offload of work from cognitive to perceptual system, expanded working memory and expanded storage of information.
- Reduced search: locality of processing, high data density and spatially-indexed addressing.
- Enhanced recognition of patterns: recognition instead of recall, abstraction and aggregation, visual schemata for organization, and enhanced patterns and trends.
- Perceptual inference: visual representations make some problems obvious, and complex specialized, graphical computations can be enabled.
- Perceptual monitoring: visualizations can allow monitoring of a large number of potential events.
- Manipulation medium: visualizations can allow exploration of a space of parameter values and amplify user operations.

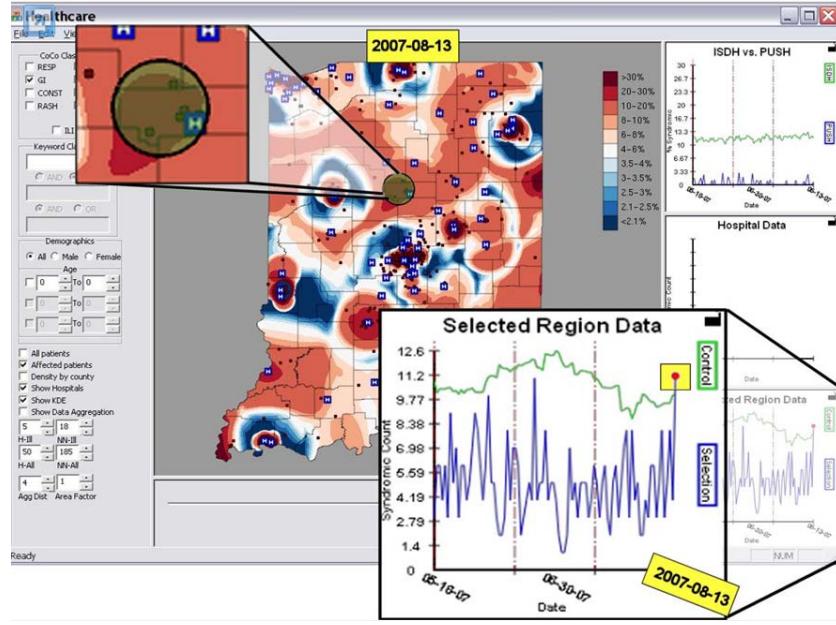
## 3 Advanced VA Concepts and Techniques Examples

This section presents some VA concepts applied to various information types. Research results are presented to illustrate the use of VA techniques.

### 3.1 Geospatial Analysis

A great amount of data to be analyzed involves a geographical component. Geospatial information has a strong mapping to spatial dimensions and usually requires the use of map displays. The complexity of datasets that also contain temporal and thematic attributes poses significant visualization challenges. If they are simple enough, these aspects can be represented using overlays, colours, textures and symbols, or by adding a third dimension axis. When the data is too complex to use a map display only, multiple linked views allow the use of a variety of representations for which the relationship with the geospatial data is shown through user interactions such as selection and filtering.

The Purdue University Regional University Visualizations and Analytics Center (PURVAC) developed a healthcare visual analytics suite of tools for spatio-temporal exploration of multivariate health care data sets in linked statistical and geospatial-temporal views (Maciejewski et al., 2008). The visual analytics environment called linked animal-human visual analytics (LAHVA) uses visual analytics for hypothesis testing in syndromic surveillance (Figure 6).



**Figure 6: LAHVA, with exploded views added. The user has selected an area of interest, generating a time series plot for that region (Maciejewski et al., 2008).**

### 3.2 Graph, Link and Network Visualization

In network information, be it a graph or a hierarchical representation, the relevant aspect is mainly the links between the data elements. However, in many situations, the number of links can quickly grow and result in an undecipherable mesh of data relationships. Innovative visualizations are required to untangle these spider webs of links and make sense of the information presented.

NodeTrix is a hybrid approach to social network visualization (Henry et al., 2007). Node-link diagrams are used to show the global structure of a network, while arbitrary portions of the network can be shown as adjacency matrices to better support the analysis of communities. It is especially useful in the case of globally sparse but locally dense social networks (Figure 7).

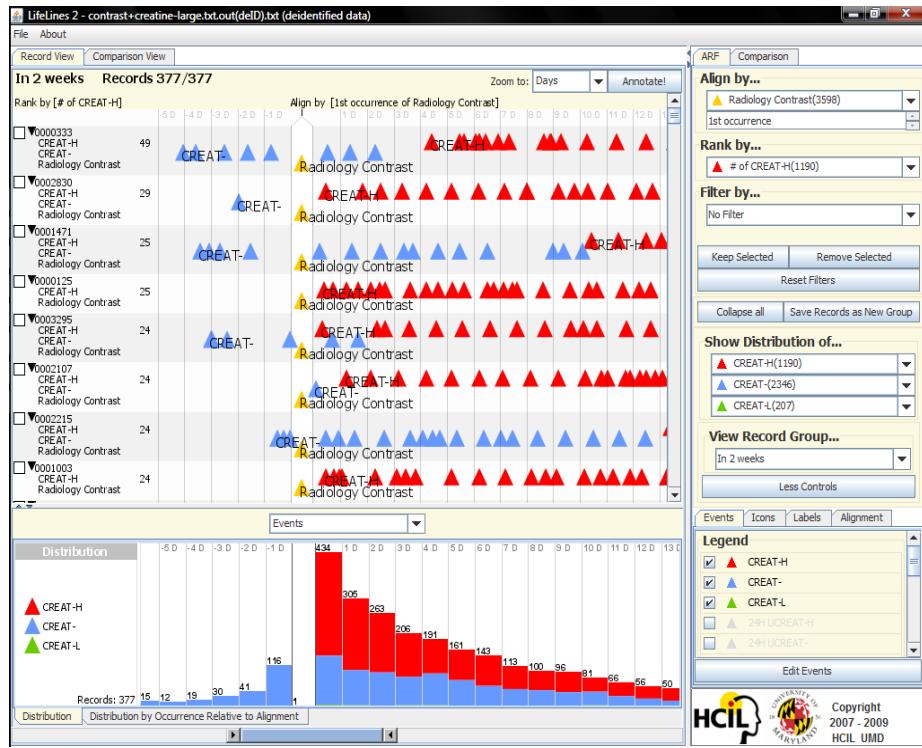


**Figure 7: NodeTrix social network visualization (Henry et al., 2007).**

### 3.3 Temporal Visualization

Temporal data analysis is useful to detect trends and recurring events over time. The study of event sequences also enables the identification of links between individual observations and possible causes for some events. The use of timelines provides an overview of what happened in a given time interval while a time slide can be used to show unfolding events in ascending or descending time order. Time sliders are especially effective when we are faced with multiple dimensions that must be represented, as is the case when combining geospatial and temporal data, for example.

Electronic records contain a wealth of information regarding categorical event data such as complaints, diagnoses and treatments. Lifelines 2 (Wang, 2010) is an interactive visualization tool that organizes this information in a temporal display to allow the discovery of patterns across multiple records, hypothesis generation and finding cause-and-effect relationships in a population (Figure 8).



**Figure 8: Lifelines2 visualization of multiple electronic health records. It contains a temporal summary, showing the distribution of the three event types over time. The control panel lets the user align all the patient records by their 1<sup>st</sup> occurrence of radiology contrast and rank them with the most number of creatine high (Wang, 2010).**

### 3.4 Multimedia Analysis

The amount of multimedia content is ever-growing. This content comprises 95% of the current digital universe and will soon grow to over 99% (Thomas, 2009).

An interesting research project (Ribarsky, 2009) that exploits news feeds is presented in Figure 9. It shows the events importance in the news over time. Topics are extracted from fused video, audio and closed captions. Since viewing video streams consumes a lot of time, a tool like this one can be very useful for the identification of relevant multimedia documents. The methods break the news broadcast streams into separate stories. The flow of follow-on stories caused by a significant event can also easily be tracked.

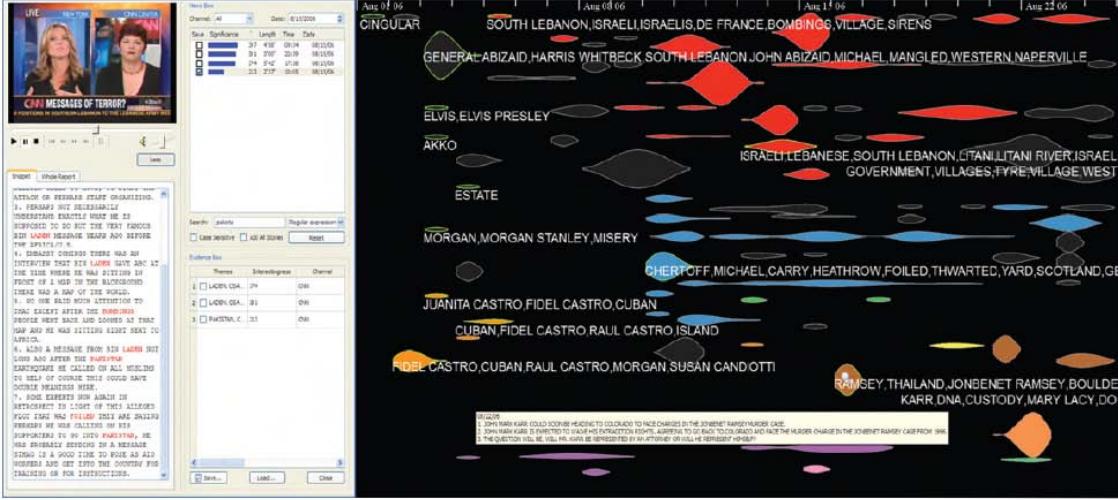


Figure 9: The EventRiver interface shows the events stream over time (Ribarsky, 2009).

### 3.5 Multivariate Visualization

Datasets with more than 3 dimensions can be very difficult to represent. A few techniques were developed in order to reduce the dimensionality of the data while being able to show the important characteristics of the datasets.

The Dust & Magnets metaphor represents individual cases as particles of iron dust, and dataset variables are represented as magnets (Soo Yi et al., 2005). This enables the user to manipulate the magnets and see the dust particles move accordingly. When a magnet is dragged, individual dust particles are attracted to the magnet based on the value of the attribute corresponding to the magnet. The dataset characteristics are exposed through the interaction with the magnets, thus enabling the user to get a feel of the importance of each variable and of the relations between them (Figure 10).

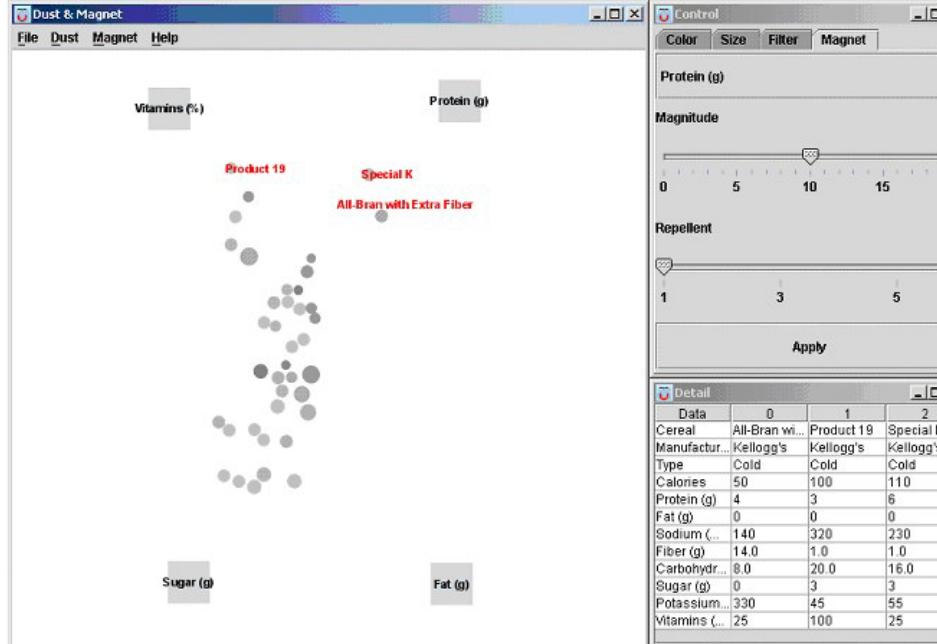


Figure 10: Dust & Magnet example using a cereal dataset (Soo Yi et al., 2005).

### 3.6 Validation and Evaluation

Evaluation of user interfaces is very challenging. Relatively little effort has been devoted to this aspect up to now in comparison to the work done in the development of tools. As more and more visual analytics applications appear, researchers are looking for a better assessment of their effectiveness and utility. The ultimate goal is the creation of a set of metrics that could predict the efficiency of tools for given tasks.

While waiting for these metrics to be defined, we can use a number of alternative methodologies and approaches. It is possible to classify them in two categories: analytic and empirical evaluations. Analytic evaluations such as heuristic inspection and cognitive walkthrough are based on formal analysis models and conducted by experts. Empirical evaluations consist of studies where measurements take place in controlled experiments and qualitative studies where data is gathered with focus groups or interviews.

The Scientific Evaluation Methods for Visual Analytics Science and Technology (SEMVAST) project focuses on two activities: making benchmark data sets available through the Visual Analytics Benchmarks Repository and seeding an infrastructure for evaluation. The VAST Challenge serves as a testbed for these activities (see section 5.5).

### 3.7 Learning More

Two very useful resources for learning more about visual analytics are the InfoVis:Wiki project (InfoVis:Wiki, 2011) and the Visual Analytics Digital Library (VADL, 2011).

## 4 Defence and Security Domains

### 4.1 Maritime Awareness

Maritime applications have a strong geospatial component and visualization of this aspect is critical to Maritime Domain Awareness (MDA). In this section, we present research projects that are specifically designed for a maritime purpose.

“Maritime Domain Awareness is the effective understanding of everything on, under, related to, adjacent to, or bordering a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, vessels, or other conveyances” (NSPD/HSPD, 2004). Maritime domain operators/analysts around the world typically have a mandate to be aware of all that is happening in maritime approaches. This mandate is based on the need to protect from attack, defend sovereignty, detect illegal activities, and support search and rescue activities.

Many complementary aspects are of interest in maritime traffic monitoring. One is the conventional overview of spatial trajectories that helps users to perceive traffic evolution for surveillance purposes. The ability to drill down in details and study specific vessels properties for particular cases of interest is also very important. Trend visualization and analysis can help detect patterns in how external factors such as economic influences or meteorological conditions affect the maritime activities or sensor performance.

Because MDA has a large mandate, there are many ways it can be improved using visual analytics. Visual spatiotemporal analysis can help detect trends as shown in the study of Somali pirate attacks. The 3D perspective map in Figure 11 illustrates the relative spatial density of reported pirate incidents in the Gulf of Aden for 2008. Analysis of this visualization showed that the attack pattern changed in response to the creation of the Maritime Security Patrol Area.

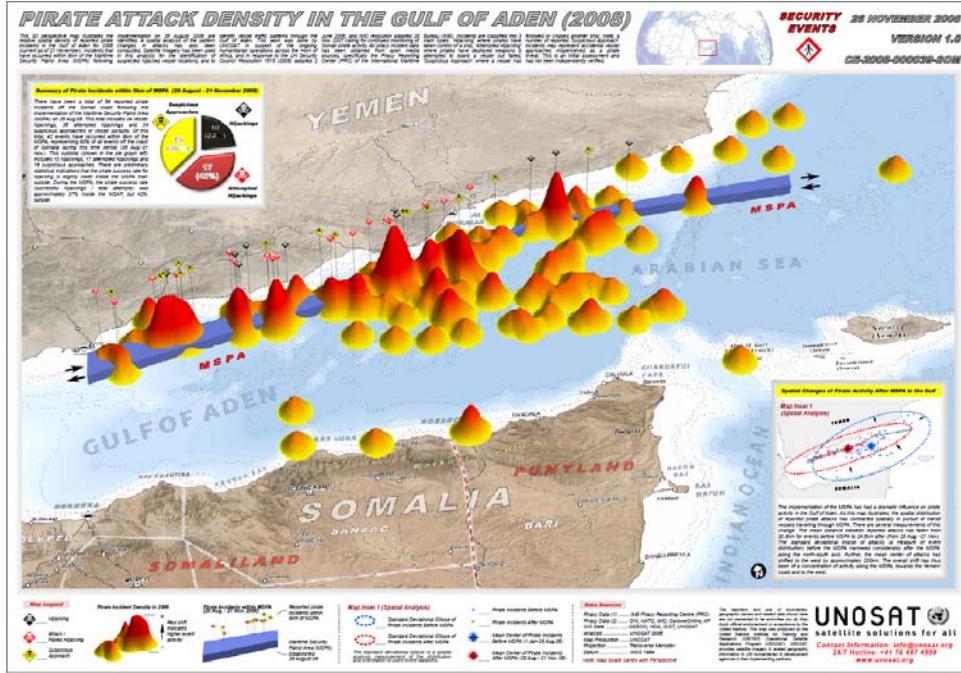


Figure 11: Visualization of pirate attacks evolution over time in the Gulf of Aden (UNOSAT, 2008).

Riveiro et al. (2008a, 2008b) built a prototype maritime application for anomaly detection in the maritime surveillance domain. It contains three areas: geographic map, detailed information and alarms list, and controls for filter, detector and vessels view. Vessels are displayed using different icons according to their type and their tracks are partially displayed to show positions reported in the last hour. Thus, longer tracks indicate high speed. A colored ellipse indicates a vessel that is flagged as anomalous and the color indicates the probability of the anomaly.

Oculus GeoTime is a commercial visual analytics application that provides the ability to track targets, show communications and relationships, and see behaviours in time and space within a single, interactive 3D display (Kapler et al., 2008). Events are represented in an X,Y,T coordinate space in which the X,Y plane shows geography and the vertical T axis represents time. Figure 12 depicts a maritime rendezvous detection using GeoTime.

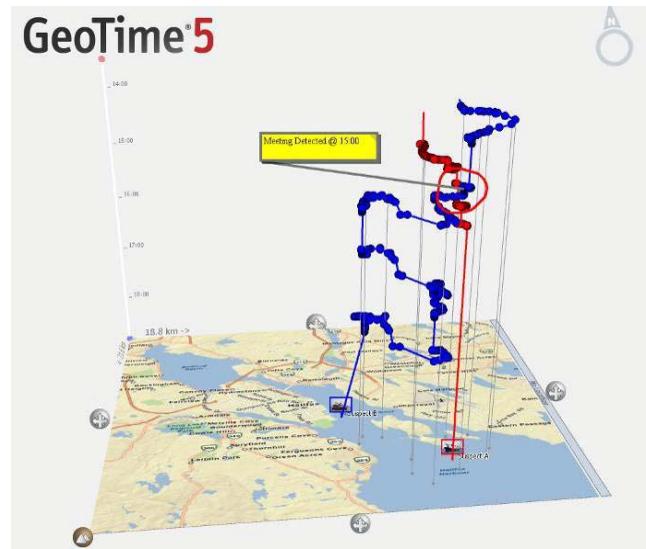


Figure 12: Maritime rendez-vous detection example in GeoTime (Oculus Info Inc).

Various vessel trajectories visualizations have been studied by Willems et al. (2008, 2009). They use historical data to compute density fields that are then shown as illuminated height maps in Figure 13. The overlay of current vessel positions on the density fields enables a comparison between the current situation and the normal maritime behaviour.

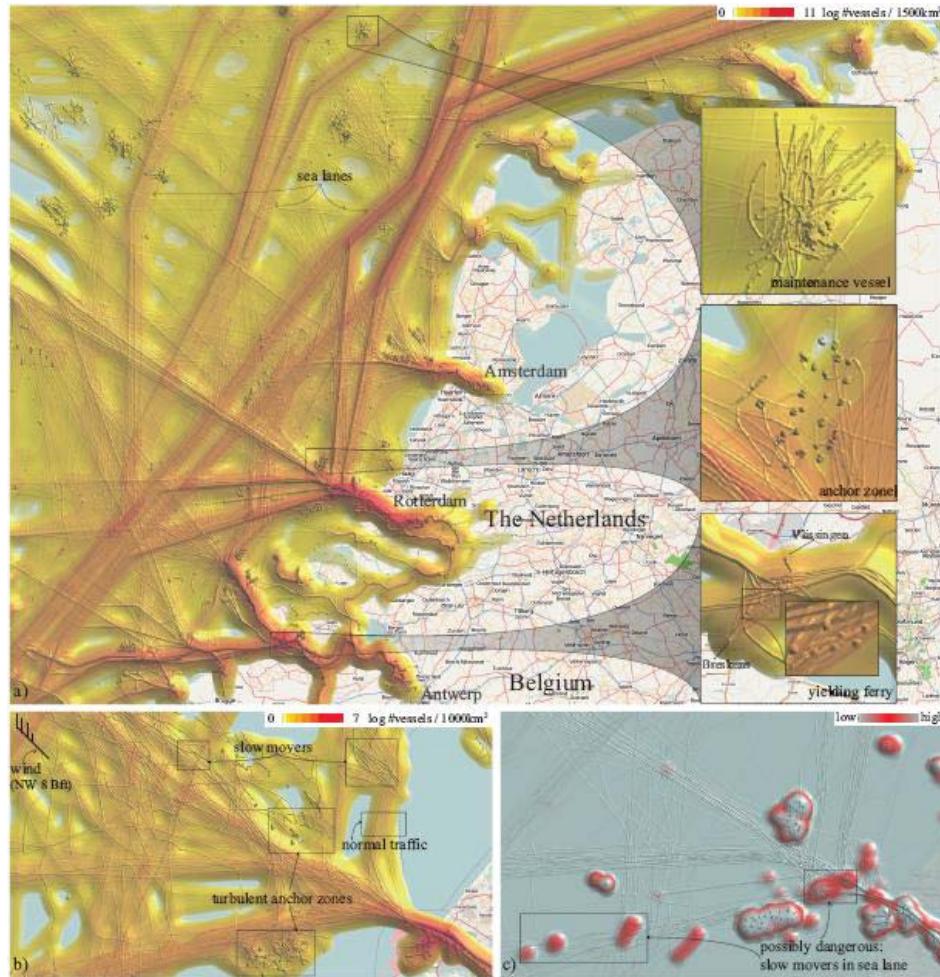


Figure 13: Visualization of vessels trajectories (Willems et al., 2009).

## 4.2 Military Intelligence

The purpose of intelligence is to provide commanders and staffs with timely, relevant, accurate, predictive, and tailored intelligence about the enemy and other aspects of the area of operations. Intelligence supports the planning, preparing, execution, and assessment of operations (HDA, 2010).

A key process for Military Intelligence is called the Intelligence Preparation of the Battlefield (IPB). It is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain and weather, and civil considerations in a specific area of interest and for a specific mission.

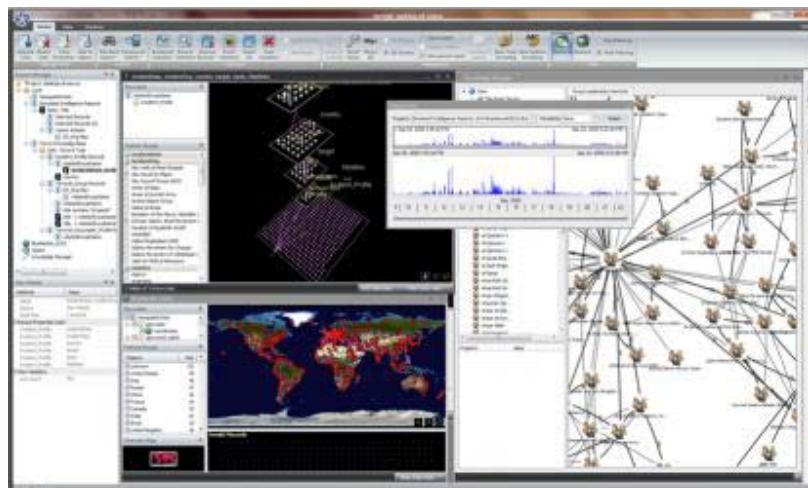
In modern conflicts, Intelligence activities are more and more concerned with Counter-Insurgency (COIN). COIN is defined as “a part of a wider set of irregular activities and threats to a secure and stable environment”. An irregular activity may be defined as: “behaviour that attempts to effect or prevent change through the illegal use, or threat, of violence, conducted by

ideologically or criminally motivated non-regular forces, groups or individuals, as a challenge to authority" (DND/CF, 2008).

In IPB and in support of COIN, information must be gathered and produced about:

- Enemy forces (Red SA), as force structure, order of battle, intent;
- Friendly forces (Blue SA) such as force structure, disposition;
- Terrain (Brown SA), such as topography, weather, hydrography, vegetation, road network;
- Neutral forces (White SA) such infrastructures, civilian institutions, populations, leaders.

In order to solve complex, multifaceted, real-world problems, intelligence analysts need to develop an understanding of various collections of data and link together information of different types. Starlight Visual Information System is a visual analytics platform where viewers can interactively move among multiple representations of the information. The use of Starlight for intelligence analysis is depicted in Figure 14. This platform enables the visualization of multiple data collections simultaneously in order to uncover correlations that may span multiple relationship types, including networks, geographical data and textual information.

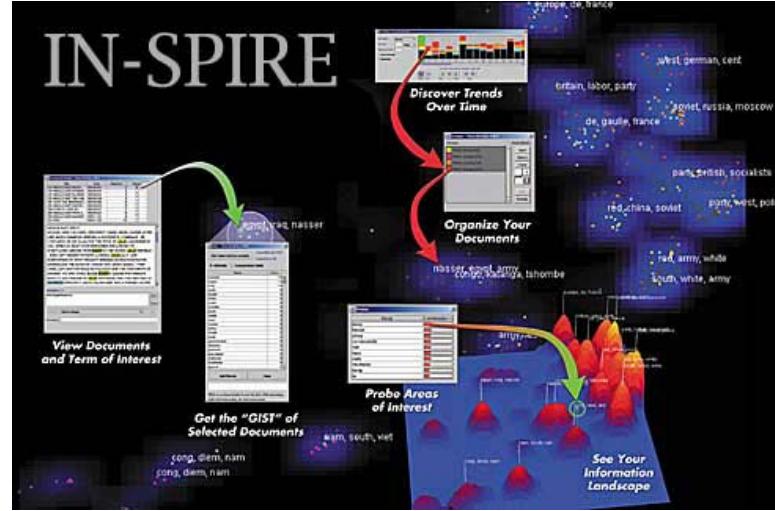


*Figure 14: Use of Starlight for intelligence analysis (Future Point Systems, 2011).*

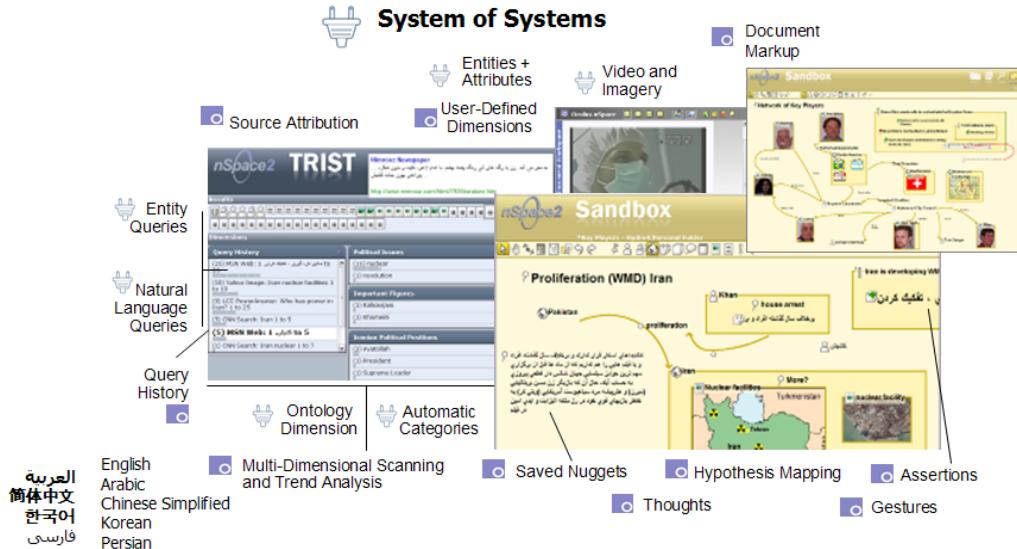
Analysts are also often faced with large collections of unformatted text documents. IN-SPIRE is a text analysis and visualization software that can quickly reveal important information from these datasets and accelerate subsequent investigation and discovery. IN-SPIRE's two main visualizations display representations of the documents in which those with similar or related topics appear closer together (Figure 15). In the Galaxy visualization (upper right), dots represent documents and cluster around center points that represent central topics or themes. In the ThemeView visualization (lower right), users see a relief map where the highest peaks represent the most prevalent topics in the collection.

Oculus nSpace is a web browser-based system of systems for intelligence analysis meant to support multiple analytical styles and workflows (Wright et al., 2006). It is the combination of two capabilities called: TRIST and Sandbox (see Figure 16). TRIST's multi-dimensional linked views help users find relevant documents (unstructured text, images, videos, etc) from web services. Queries can be saved and scheduled to be executed repeatedly. The Sandbox is a space where relevant information can be dropped and where analytical sense making happens. Elements can be grouped and collapsed. Graphs and networks are supported and matrices allow analysis of

competing hypotheses using groups of evidence. The Sandbox supports flexible visual cognition through spatial arrangement.



*Figure 15: The IN-SPIRE discovery tool integrates information visualization with query and other interactive capabilities (PNNL 2011).*



*Figure 16: Oculus nSpace TRIST and Sandbox capabilities (Oculus Info Inc).*

### 4.3 Cyber Warfare

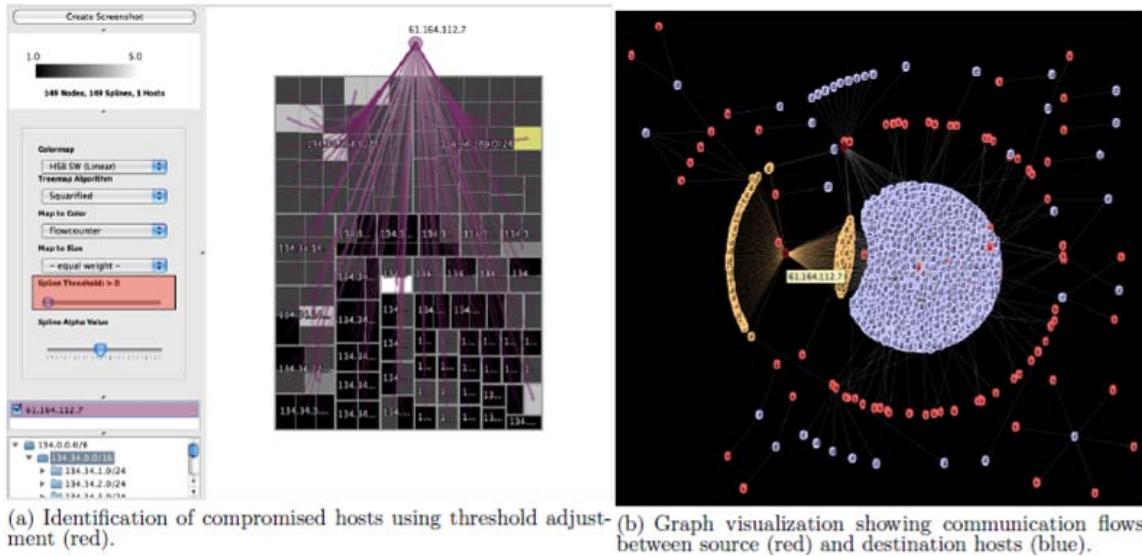
As the modern world is relying heavily on computers and networks to conduct day-to-day activities, these computers and networks have become increasingly a target of choice for countries conducting spying or disruptive operations, terrorist and criminal organizations or simply hackers. The impact of cyber attacks on a country, an organization or individuals can be severe and costly. Moreover, network attacks are increasingly sophisticated and unpredictable.

Good security tools are necessary to properly manage computer networks, prevent and detect intrusions. This includes tools to analyze service usage in a network, detect a distributed attack, and investigate hosts in a network that communicate with suspect external IPs. One key requirement for these tools is the ability to process and filter massive amounts of information.

Visual analytics techniques have been explored and put in service to counter cyber warfare. “Visualization is often appropriate when human intelligence and domain knowledge must be combined with automated methods. This is certainly the situation with monitoring and exploring network traffic patterns. The sheer number of alerts and the sophistication of attacks requires a symbiosis of Intrusion Detection Systems (IDS) algorithms and human analysis to fight new adversaries” (Mansmann et al., 2009).

The visual analytics applications used in cyber warfare are mostly related to network analysis. The NFlowVis Network visualization tool provides a number of views used to perform large-scale network traffic monitoring and to analyse intrusion detection events. For example, as shown on Figure 17a, a TreeMap is used to represent compromised hosts in the center of the display and selecting attacking hosts arranged at the borders of the display. Figure 17b, is a graph visualization showing communication flows between source and destination hosts.

Starlight (see section 4.2) can also be used for cyber security and computer forensics. The use of Starlight for cyber network analysis is depicted in Figure 18.



(a) Identification of compromised hosts using threshold adjustment (red).

(b) Graph visualization showing communication flows between source (red) and destination hosts (blue).

Figure 17: Example of NFlowVis (Mansmann et al., 2009).

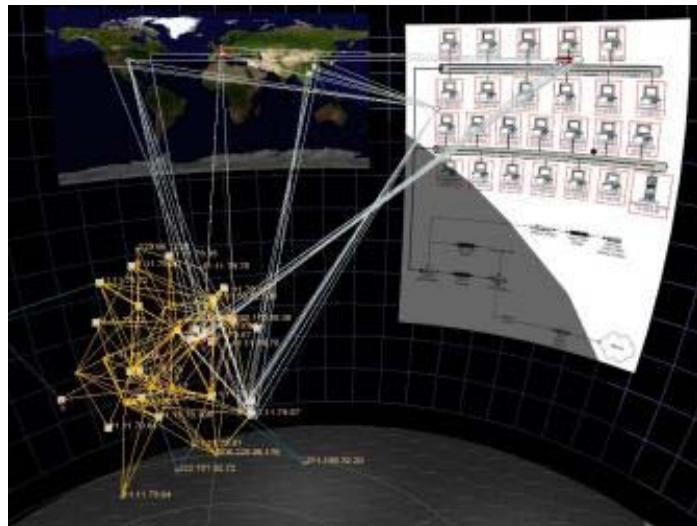


Figure 18: Use of Starlight for cyber analysis (Future Point Systems, 2011).

## 4.4 Emergency Management

Emergency management refers to a wide range of measures to protect communities and the environment from risks and to recover from emergency events stemming from either natural or human-induced causes.

Through legislation and government policy, Public Safety Canada, which was created in December 2003, is responsible for leading by coordinating the management of emergencies among federal departments and agencies. This includes establishing policies and programs for the preparation, testing and exercising, and implementing emergency management plans. It also includes monitoring and coordinating a common federal approach to emergency response along with the provinces, resulting in an “all-hazards” approach incorporating prevention and mitigation, preparedness, response, and recovery. The department’s responsibility for emergency management includes coordinating the protection of critical infrastructure, from planning for emergencies to recovering from them. Critical infrastructure includes physical and information technology facilities, networks, services, and assets essential to the health and safety or economic well-being of Canadians (OAG, 2009).

The Multi-Agency Situational Awareness System is the result of a Canadian national R&D initiative to provide a multi-agency (federal, provincial and territorial stakeholders) with a Common Operational Picture for emergency management. By exploiting interoperability standards, it is expected that this system will allow for the timely sharing of geospatial referenced information (Figure 19). It is funded through the GeoConnections and the Centre for Security Sciences (CSS), Public Security Technical Program (PSTP).



Figure 19: Multi-Agency Situation Awareness System.

The US Department of Homeland Security and Pacific Northwest National Laboratory (PNNL) developed a vision of future work environments for the emergency management community (IVAC, 2010). Called Precision Information Environments (PIEs), these environments are meant to provide planners and responders with precise, relevant information and with tools that aid collaboration, information sharing, and decision support (DHS/PNNL, 2010). A video illustrating the concepts of a PIE environment to support fire fighters has been developed (DHS/PNNL, 2010). Figure 20 shows snapshots from the video. The visual interfaces presented in this video are cleverly designed, including important aspects that are often ignored such as uncertainty visualization. One of the key VA concepts illustrated in the PIE is the adaptive user interface: user models define the roles, responsibilities and perspectives of each person using a PIE. Software interfaces adapt their form to support each user's tasks and preferences. They represent a powerful tool to support the cognitive aspects of emergency management tasks.



Figure 20: Precision Information Environments Wild Fire Vignette video snapshots (DHS/PNNL 2010).

## 5 Key Organizations and Initiatives

### 5.1 Visualization and Analytics Community (VAC)

Visual analytics is not only a research field, it is also a community. The Visual Analytics Community (VAC) is comprised of people and organizations from around the world who are stakeholders in the advancement and application of visual analytics technology. The VAC brings together diverse individuals and organizations from academia, government, and industry. At the core of this community is the VAC Consortium. It is an international consortium of individuals,

institutions, and government agencies that acts as focal point and champion for addressing the diverse needs of the Visual Analytics Community, including user, research and application development, business, and educational needs. A consortium meeting is held annually. The event includes talks from government and industry experts, research highlights, product demonstrations, and discussions with leaders in the field of visual analytics.

## 5.2 NVAC, CNVAC, UKVAC and VisMaster

Without any doubt, the most active organization in visual analytics is the US National Visualization and Analytics Center (NVAC) which was the first to establish the nature, scope, and importance of VA (Thomas and Cook, 2005). Today, visual analytics R&D has expanded well beyond the US borders as shown in Figure 21. In Canada, there is a Canadian Network of Visualization and Analytics Centers (CNVAC). UK has a similar network called UK Visual Analytics Consortium (UKVAC). VisMaster (Kohlhammer and Keim, 2007) is a European Coordination Action Project focused on the research discipline of visual analytics which consists of 37 partners from 13 different countries.



*Figure 21: Visual analytic collaborations and organizations involved in the Visual Analytics Community (VAC) from the US viewpoint (VAC Views, 2010).*

## 5.3 US Homeland Security Centers of Excellence

The Homeland Security Centers of Excellence conduct multidisciplinary research and education for homeland security solutions. Each center is led by a university in collaboration with partners from other institutions, agencies, laboratories, think tanks and the private sector. There are currently 12 Centers of Excellence across the US and 5 of them are part of the VAC.

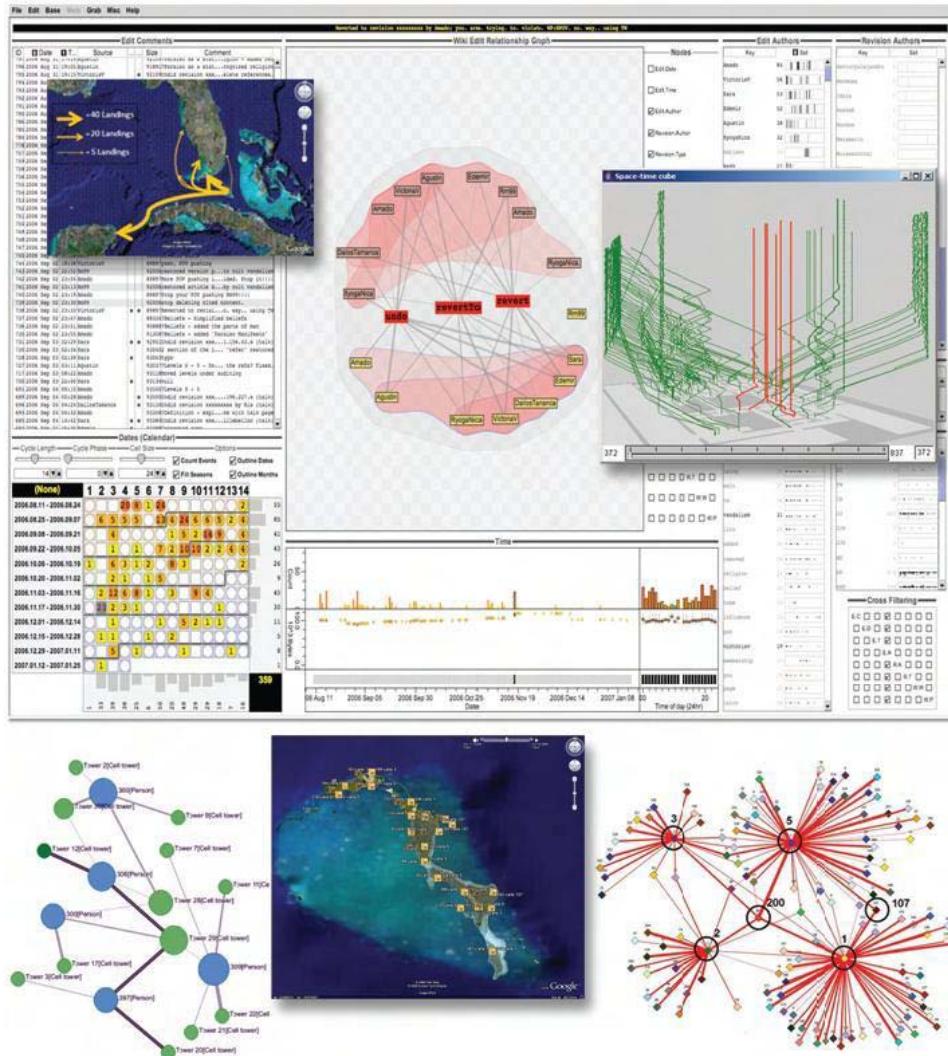
## 5.4 Resources

VAC Views is a biannual publication that provides information about different visual analytics applications, outreach efforts including recent and upcoming conferences and workshops, and educational highlights.

The visual analytics community social website, vacommunity.org, was created in 2010 and is meant to act as a coordination point where each community of research and practice has access to dedicated blogs, forums, wikis, calendars, RSS feeds for information distribution, and other social media services. The iVAC.org site was also created in 2010. It will provide formal news, information, and articles on visual analytics to broaden the outreach of the Integrated Visualization and Analytics Community (iVAC).

## 5.5 VAST Challenges

The VAST Challenge is an original mean of gathering visual analytics developers and researchers around shared benchmark datasets and comparing new visual analytics tools. It is proposed every year to the international VA community as part of the IEEE VAST Symposium. Participants can demonstrate the visual analytics capabilities of their tools against an invented scenario and synthetic datasets. The challenge scenario and datasets then remain available to anyone interested in testing their VA tools with representative tasks and datasets. Figure 22 shows visualizations that were submitted to the VAST 2008 Challenge.



**Figure 22: Visualizations submitted to the VAST Challenge 2008, from (clockwise, from upper left): SPANDAC, NEVAC, Fraunhofer Institute, Ocularis Info Inc., Palantir, Ocularis Info Inc (VAC Views, 2009).**

## 6 Conclusion

In the context of modern defence and security operations, analysts are faced with significant data overload problems which prevent them from understanding a situation at hand and anticipating how this situation may develop. Fortunately, VA has emerged as a significant multi-disciplinary research field that leverages the human cognitive abilities to comprehend information when presented in a proper way and combined with suitable interaction. To describe VA, this paper has presented a number of information visualization, interaction and analytical reasoning techniques that allow making the relevant information more salient in order to help detect patterns, trends and anomalies. VA is making its way into defence and security applications. Examples of this are anomaly detection in the maritime domain; making sense out of large collections of unformatted text documents for military intelligence analysis; performing large-scale network traffic monitoring and intrusion detection in the cyberspace domain; and developing proper situation awareness during an emergency management crisis. VA has a significant momentum and VA research and applications have been growing exponentially over the last years. Several VA applications have become available commercially, various key communities have been stood up and significant initiatives have been undertaken.

## 7 References

Card, S.K., Mackinlay, J.D. and Shneiderman, B. (1999), *Readings in Information Visualization: Using Vision to Think*, Morgan Kaufmann Publishers, San Francisco, 1999.

Card, S. K., Robertson, G. G. and Mackinlay, J. D. (1991), The Information Visualizer: An Information Workspace, In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'91), pp. 181-186, ACM Press, New York.

DHS / PNNL (2010), Precision Information Environments, <http://precisioninformation.org/>, retrieved Janauray 2011.

DND/CF (2008), Counter-Insurgency Operations B-GL-323-004/FP-003, 2008.

Future Point Systems, Inc (2011), <http://www.futurepointsystems.com/>, retrieved May 2011.

Headquarters Department of the Army (2010), Field Manual (FM) 2-0: Intelligence, Washington, DC, 23 March 2010, <http://www.fas.org/irp/doddir/army/fm2-0.pdf>, retrieved January 2011.

Healey, C. G. (2009), Perception in Visualization, last updated 11-May-2009, from Christopher Healey's web site: <http://www.csc.ncsu.edu/faculty/healey/PP/index.html>, retrieved September 2009.

Henry, N., Fedeke, J.-D. and McGuffin, M. (2007), NodeTrix: a Hybrid Visualization, IEEE TCGV, Proceedings Visualization/Information Visualization 2007.

InfoVis:Wiki (2011), [http://www.infovis-wiki.net/index.php/Visual\\_Analytics](http://www.infovis-wiki.net/index.php/Visual_Analytics), retrieved January 2011.

IVAC (2010), PIE Concept Video and Community Website Released, <http://www.theivac.org/content/pie-concept-video-and-community-website-released>, retrieved January 2011.

Kapler, T., Eccles, R., Harper, R. and Wright, W. (2008), Configurable Spaces: Temporal Analysis in Diagrammatic Contexts, IEEE Visual Analytics Science and Technology (VAST 2008), October 19-24, 2008, Columbus, Ohio, USA, IEEE.

Koffka, K. (1935), *Principles of Gestalt Psychology*, Harcourt Brace, New York.

Kohlhammer, J. and Keim, D. (2007), Visual Analytics in Europe - Mastering the Information Age, [http://www.igd.fraunhofer.de/ig-a3/downloads/VA/Whitepaper\\_Visual\\_Analytics.pdf](http://www.igd.fraunhofer.de/ig-a3/downloads/VA/Whitepaper_Visual_Analytics.pdf), retrieved November 2010.

Kosara, R., Miksch, S. and Hauser, H. (2001), Semantic Depth of Field, Proceedings of IEEE Symposium on Information Visualization (InfoVis 2001), IEEE, p. 97-104.

Maciejewski, R., Rudolph, S., Hafen, R., Abusalah, A., Yakout, M., Ouzzani, M., Cleveland, W.S., Grannis, S.J., Wade, M. and Ebert, D.S. (2008), Understanding Syndromic Hotspots - A Visual Analytics Approach. IEEE Symposium on Visual Analytics Science and Technology (VAST), pp. 35-42, 2008.

Mansmann, F., Fisher, F., Keim, D.A. and North, S. C. (2009), Visual Support for Analysing Network Traffic and Intrusion Detection Events using TreeMap and Graph Representations, CHiMiT '09 Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology.

Miller, R. B. (1968), Response Time in Man-Computer Conversational Transactions. Proc. AFIPS Fall Joint Computer Conference Vol. 33, pp. 267-277.

Minard, C.J. (1869), Carte figurative des pertes successives en hommes de l'Armée française dans la campagne de Russie 1812-1813, [http://en.wikipedia.org/wiki/Charles\\_Joseph\\_Minard](http://en.wikipedia.org/wiki/Charles_Joseph_Minard), retrieved January 2011.

NSPD/HSPD, (2004), National Security Presidential Directive/Homeland Security Presidential Directive, Maritime Security Policy, NSPD-41/HSPD-13, [www.fas.org/irp/offdocs/nspd/nspd41.pdf](http://www.fas.org/irp/offdocs/nspd/nspd41.pdf), retrieved October 2010.

OAG (2009), Office of the Auditor General of Canada, 2009 Fall Report of the Auditor General of Canada.

PNNL (2011), <http://in-spire.pnnl.gov/>, retrieved May 2011.

Ribarsky, B. (2009), Multimedia Visual Analytics, VAC Views, May 09, p. 10-11.

Riveiro, M., Falkman, G. and Ziemke, T. (2008a), Visual Analytics for the Detection of Anomalous Maritime Behavior, In Banissi, E. et al. (Eds.) Proceedings of the 12th IEEE International Conference on Information Visualisation (IV'08), London, UK, July 9-11 2008, p 273-279, IEEE.

Riveiro, M., Falkman, G. and Ziemke, T. (2008b), Improving Maritime Anomaly Detection and Situation Awareness through Interactive Visualization, In Proceedings of the 11th IEEE International Conference on Information Fusion (FUSION 2008), Cologne, Germany, June 30-July 3, 2008, p 47-54, IEEE.

Shneiderman, B. (1996), The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations, Proceedings of the IEEE Symposium on Visual Languages, IEEE Computer Society Press, pp. 336-343.

Simons, D. J. and Chabris, C. F. (1999), Gorillas in Our Midst: Sustained Inattentional Blindness for Dynamic Events, Perception, 28, p. 1059-1074.

Soo Yi, J., Kang, Y. A., Stasko, J. and Jacko, J. A. (2007), Toward a Deeper Understanding of the Role of Interaction in Information Visualization, IEEE Transactions on Visualization and Computer Graphics (TVCG), 13(6). Presented in InfoVis 2007, Sacramento, California, October 28 - November 1, pp. 1224-1231.

Soo Yi, J., Melton, R., Stasko, J. and Jacko, J. (2005), Dust & Magnet: Multivariate Information Visualization using a Magnet Metaphor, Information Visualization, 4(4), p. 239-256.

Stone, M. (2006). Choosing Colors for Data Visualization, January 17, 2006, [http://www.perceptualedge.com/articles/b-eye/choosing\\_colors.pdf](http://www.perceptualedge.com/articles/b-eye/choosing_colors.pdf), retrieved March 2010.

Thomas, J.J. (2009), Visual Analytics Techniques that Enable Knowledge Discovery: Detect the Expected and Discover the Unexpected, June 28, 2009, ACM SIGKDD Workshop on Visual Analytics and Knowledge Discovery (VAKD '09), Paris, France.

Thomas, J.J. and Cook, K.A., eds. (2005), Illuminating the Path: The Research and Development Agenda for Visual Analytics, IEEE Computer Society Press, <http://nvac.pnl.gov/agenda.stm#book>, retrieved November 2010.

Tufte, E. (1990), Envisioning Information, Graphics Press, 1990.

UNOSAT, (2008), Pirate Attack Density in the Gulf of Aden, Product ID: 1298 – English, 26 Nov, 2008.

VAC Views (2010), Current and Emerging Partnerships among Academia, Industry and Government, August 2010, p.20-21, <http://nvac.pnl.gov/vacviews/>, retrieved November 2010.

VAC Views (2009), The VAST 2008 Challenge, May 2009, p.14-15,  
<http://nvac.pnl.gov/vacviews/>, retrieved May 2011.

VADL (2011), <http://vadl.cc.gatech.edu/>, retrieved January 2011.

Wang, T.D. (2010), Interactive Visualization Techniques for Searching Temporal Categorical Data, Ph.D. Dissertation from the Department of Computer Science, University of Maryland, May, 2010.

Ware, C. (2000), Information Visualization – Perception for Design, Academic Press, 2000.

Wertheimer, M. (1938), Laws of Organization in Perceptual Forms, in A Source Book of Gestalt Psychology, W. D. Ellis (ed), p. 71-88, Harcourt Brace.

Willems, N., Watering, H.v.d. and Wijk, J.J.v. (2009), Visualization of Vessel Movements, Proceedings of 11th Eurographics/IEEE-VGTC Symposium on Visualization (EuroVis 2009), Berlin, Germany, June 10 - 12, 2009, vol. 28 (3), IEEE.

Willems, N., Watering, H.v.d. and Wijk, J.J.v. (2008), Visualization of vessel trajectories for maritime safety and security systems, Interactive poster at the IEEE Information Visualization Conference (InfoVis 2008), Columbus, Ohio, USA, October 19-24, 2008, IEEE.

Wright, W., Schroh, D., Proulx, P., Skaburskis, A. and Cort, B. (2006), The Sandbox for Analysis - Concepts and Methods, ACM CHI, 2006.

# Applicability of Visual Analytics to Defence and Security Operations

## (Presentation #42)

16th ICCRTS  
Québec, 21-23 June 2011

Valerie Lavigne  
Denis Gouin  
Innovative Interfaces and Interactions Group  
Intelligence and Information Section  
DRDC Valcartier



# Presentation Plan

- Information Overload
- Introduction to Visual Analytics
- Key Organisations
- Advanced Visual Analytics Concepts
- Application to Defence and Security Operations
- Visual Analytics Resources

# Information Overload – Scale of Things to Come

- Information (IDC, 2007):
  - In 2002, recorded media and electronic information flows generated about 22 EB ( $10^{18}$ ) of information
  - In 2006, the amount of digital information created, captured, and replicated was 161 EB
  - In 2010, the amount of information added annually to the digital universe will be about 988 EB (almost 1 ZB)

IDC (2007), The Expanding Digital Universe - A Forecast of Worldwide Information Growth through 2010

Kielman, J. and Thomas, J.J. (2008), Visual Analytics: A Global Collaboration

# Information Overload – Scale of Things to Come

- Drivers of digital universe:
  - 70% of the universe is being produced by individuals
  - Organizations (businesses, agencies, governments, universities) produce 30% :
    - Walmart has a database of 0.5 PB; it captures 30,000,000 transactions/day
  - The growth is uneven
    - Today the United States accounts for 41% of the Universe; by 2010, the Asia Pacific region will be growing 40% faster than any of the other regions

IDC (2007), The Expanding Digital Universe - A Forecast of Worldwide Information Growth through 2010

Kielman, J. and Thomas, J.J. (2008), Visual Analytics: A Global Collaboration

# Information Overload – Scale of Things to Come

- Kinds of data:
  - About 2 GB of digital information is being produced per person per year
  - 95% of the Digital Universe's information is unstructured
    - 25% of the digital information produced by 2010 will be images
  - By 2010, the number of e-mailboxes will reach 2 billion
    - The users will send 28 trillion e-mails/year, totaling about 6 EB of data

IDC (2007), The Expanding Digital Universe - A Forecast of Worldwide Information Growth through 2010

Kielman, J. and Thomas, J.J. (2008), Visual Analytics: A Global Collaboration

# Visual Analytics Definition

examine evidence, infer  
meaning, test truth

“Visual analytics is the science of  
**analytical reasoning** facilitated  
by **interactive visual interfaces**.”

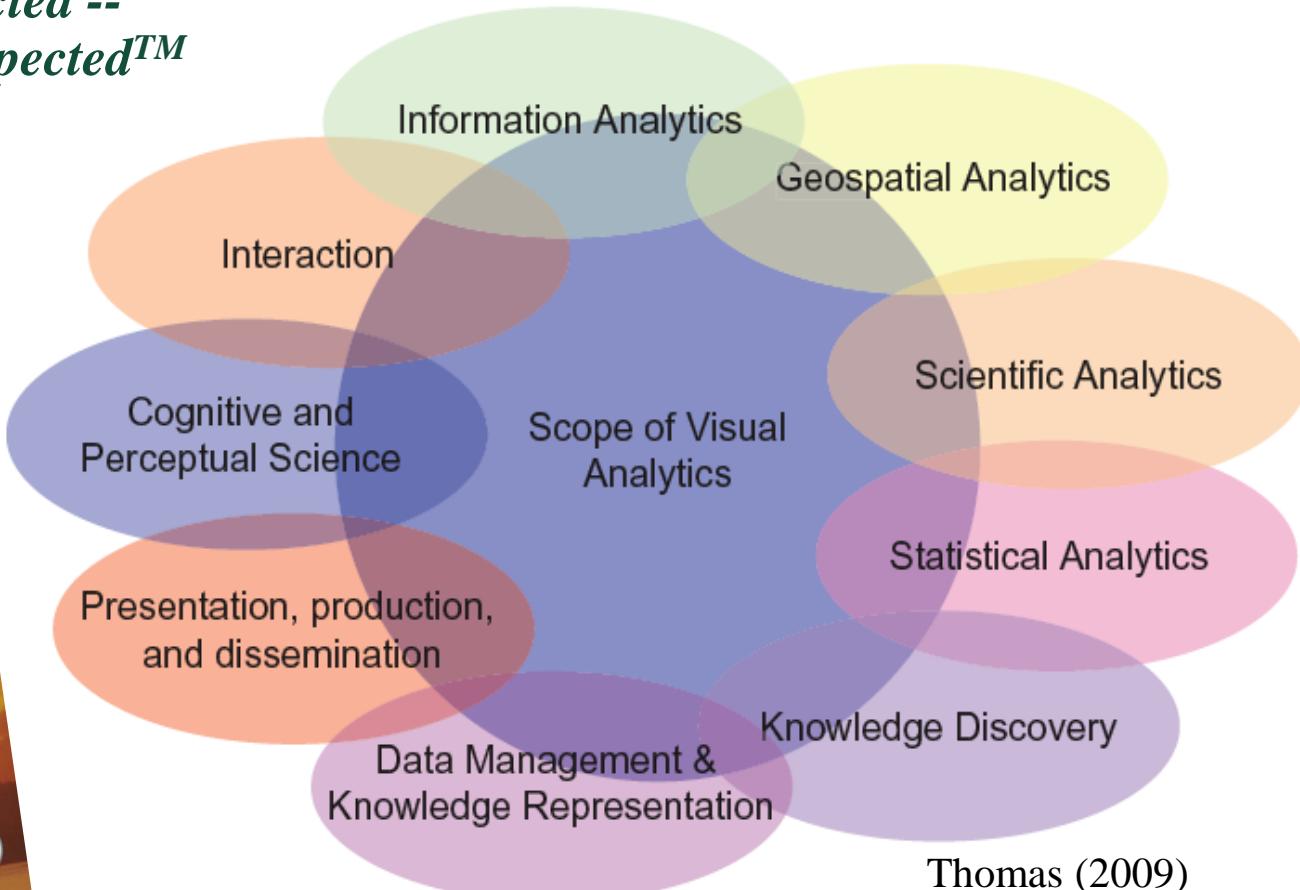
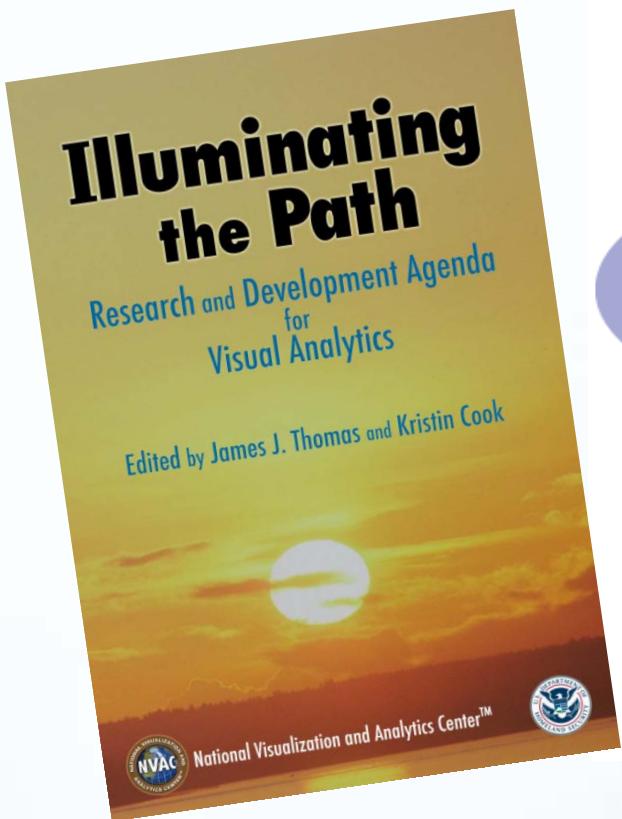
Thomas, J.J. and Cook, K.A., eds. (2005), Illuminating the Path:  
The Research and Development Agenda for Visual Analytics

ask questions, test  
hypothesis, filter results,  
explore information,  
record thinking process

take advantage of human  
brain’s aptitude for visual  
pattern recognition

# Visual Analytics R&D

*Detecting the Expected --  
Discovering the Unexpected™*



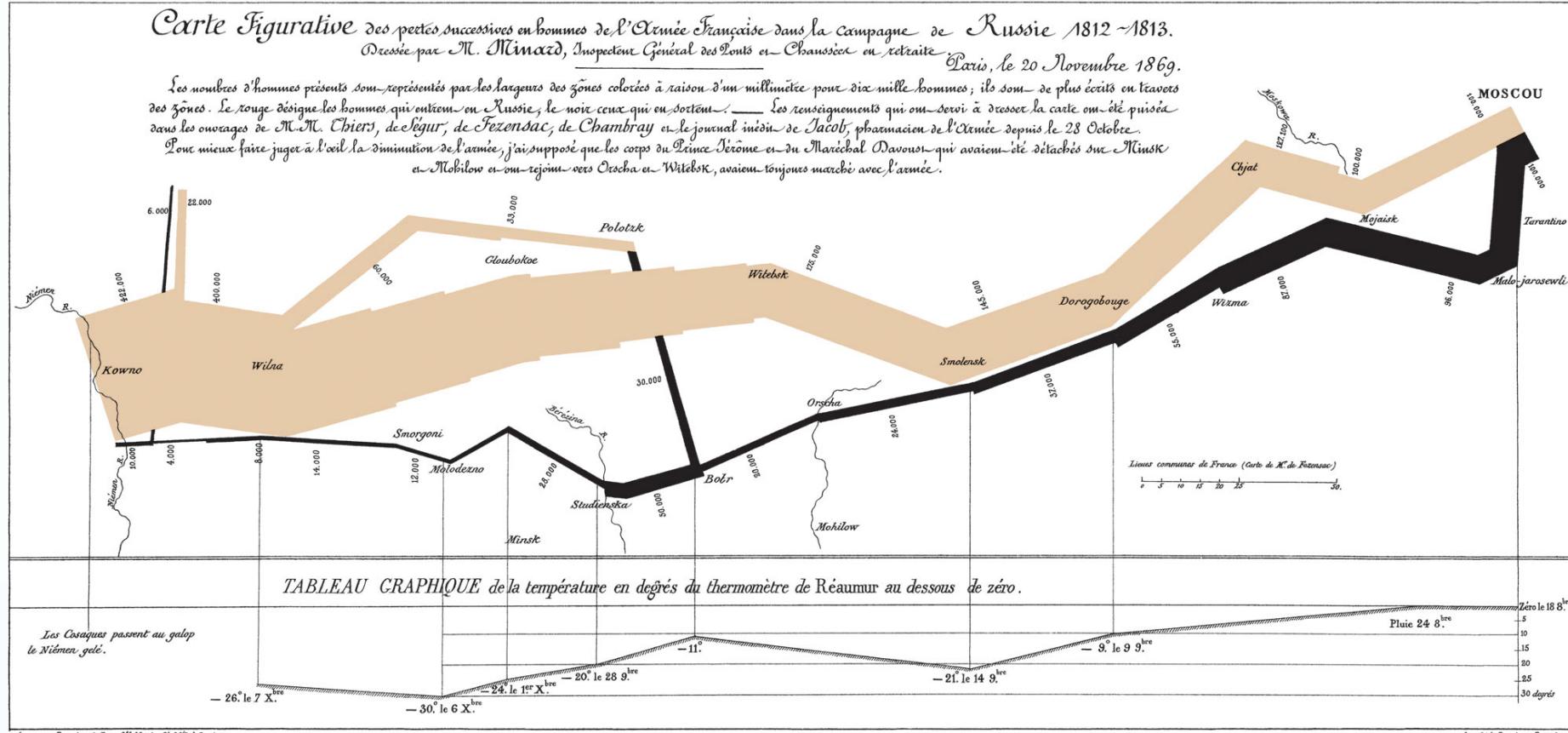
Homeland  
Security

# Key Organisations



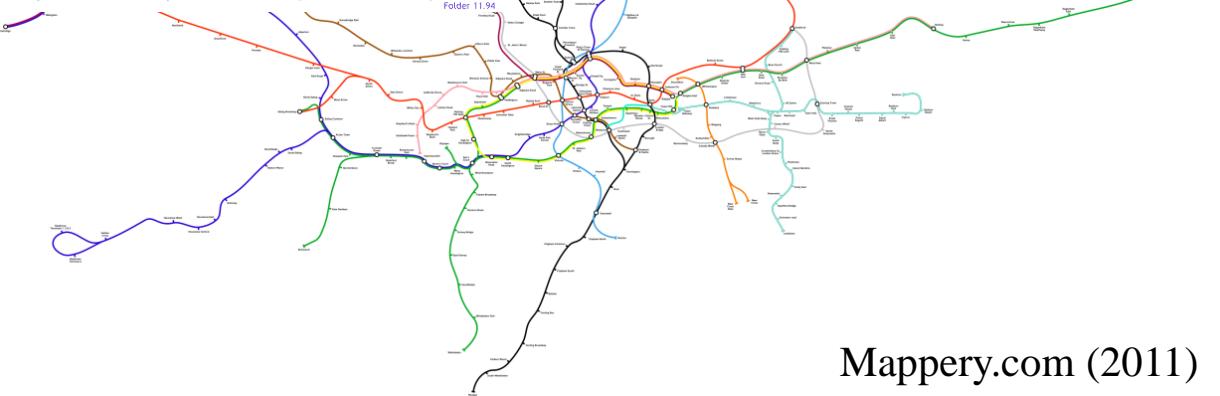
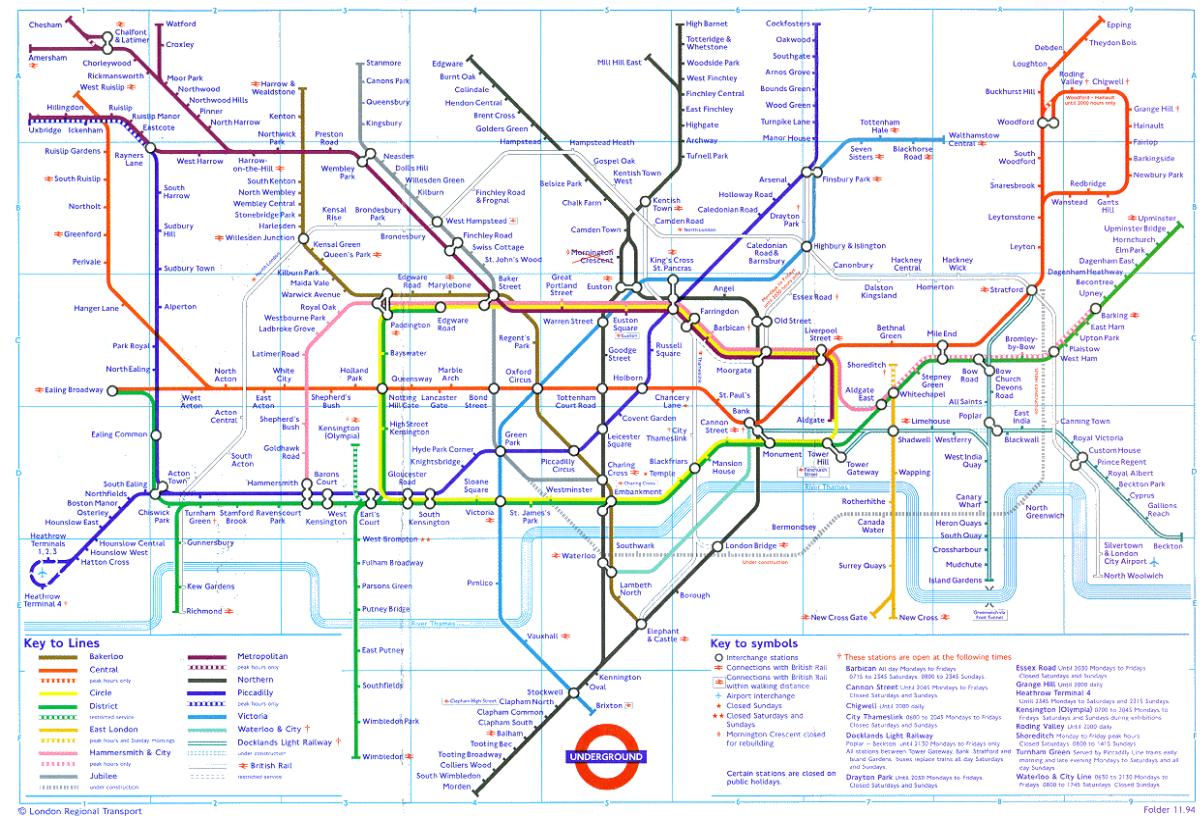
# Information Visualization

## Napoleon's Invasion of Russia

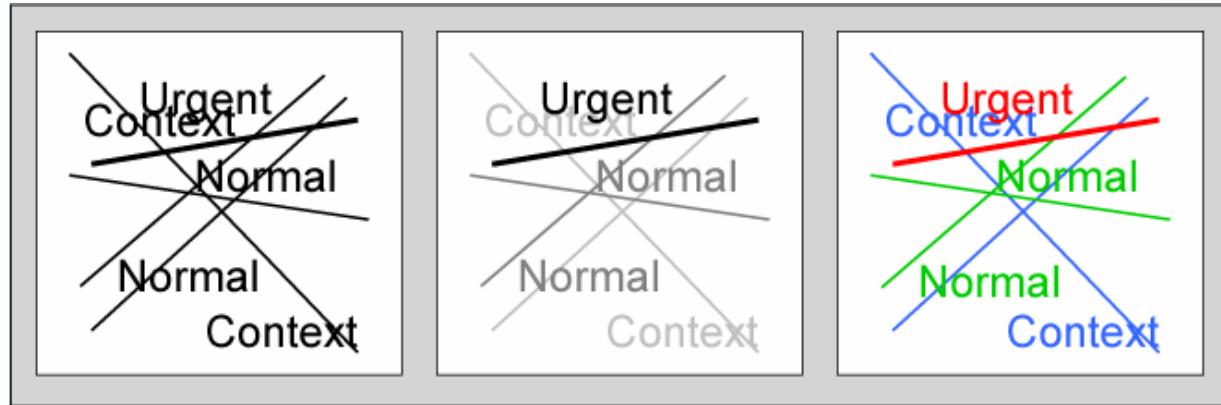


Minard (1869)

# Information Visualization: London Subway Map



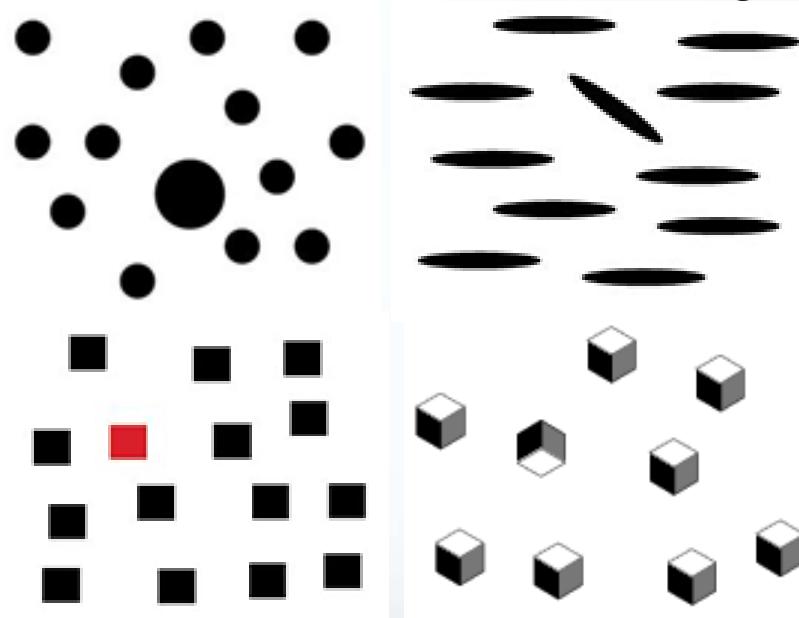
# Visual Perception



Color  
Matters

Stone (2006)

## Preattentive Processing



adapted from Healey (2009)



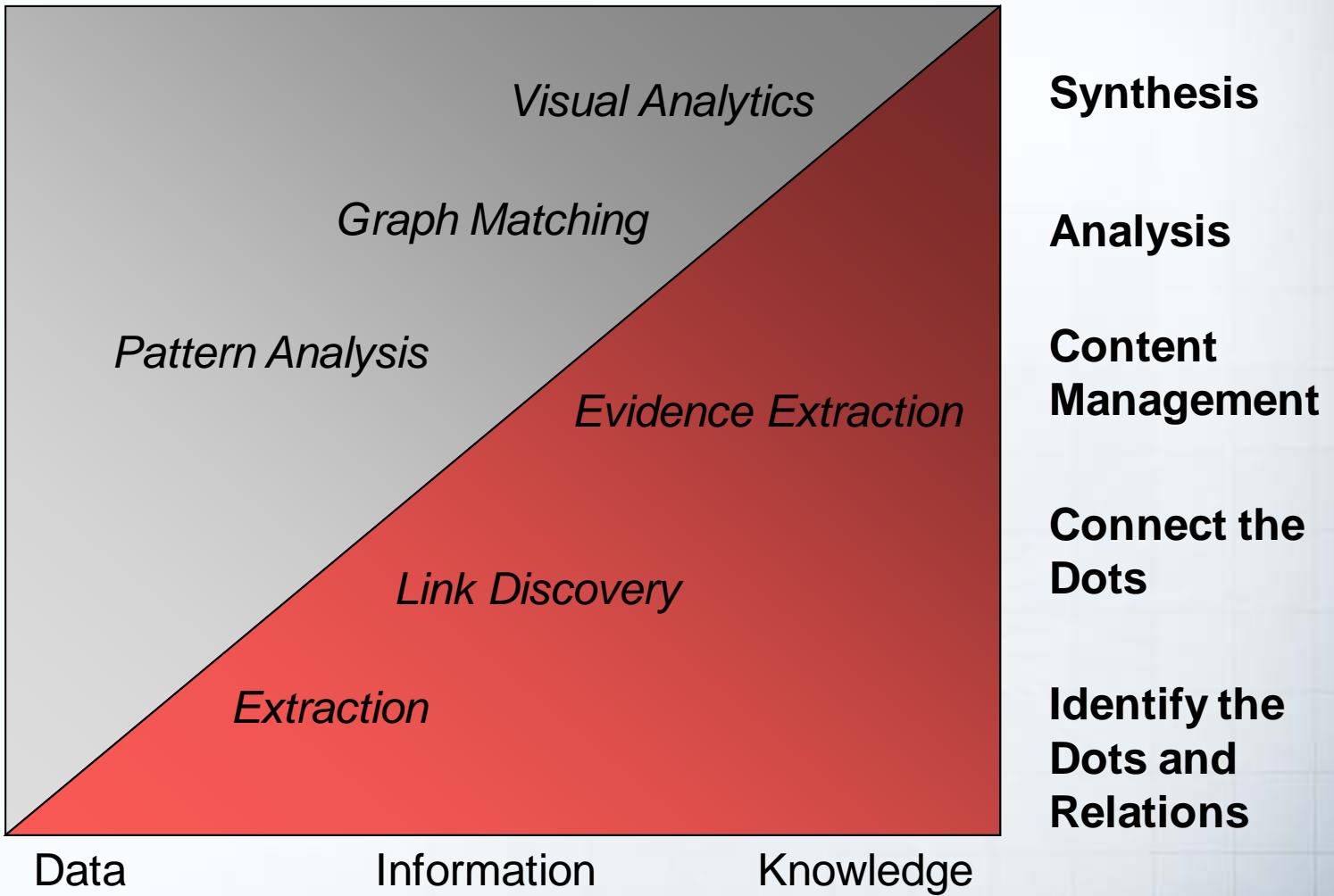
Kosara et al., 2001

# Interaction – Response Time

- Three categories of responsiveness for interactivity:  
Miller (1968), Card *et al.* (1991)
- 0.1 s : perceived as instantaneous
- 1.0 s : uninterrupted flow of thought but perceived delays
- 10 s : for delay longer than that, users will want to do something else while waiting for the computer

# Analytics

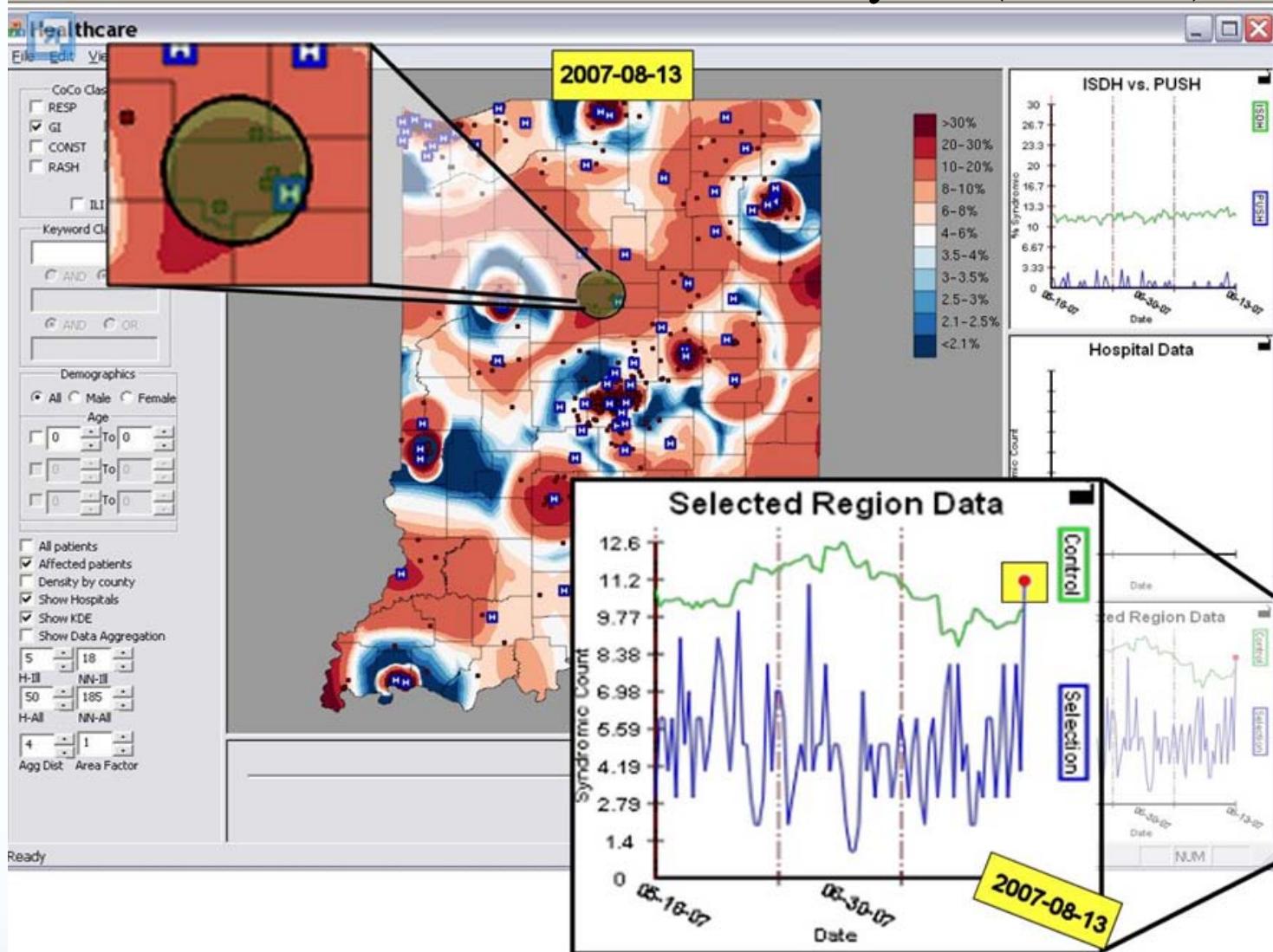
Prediction  
Cognition  
Organization  
Integration  
Aggregation



Kielman and Thomas (2008)

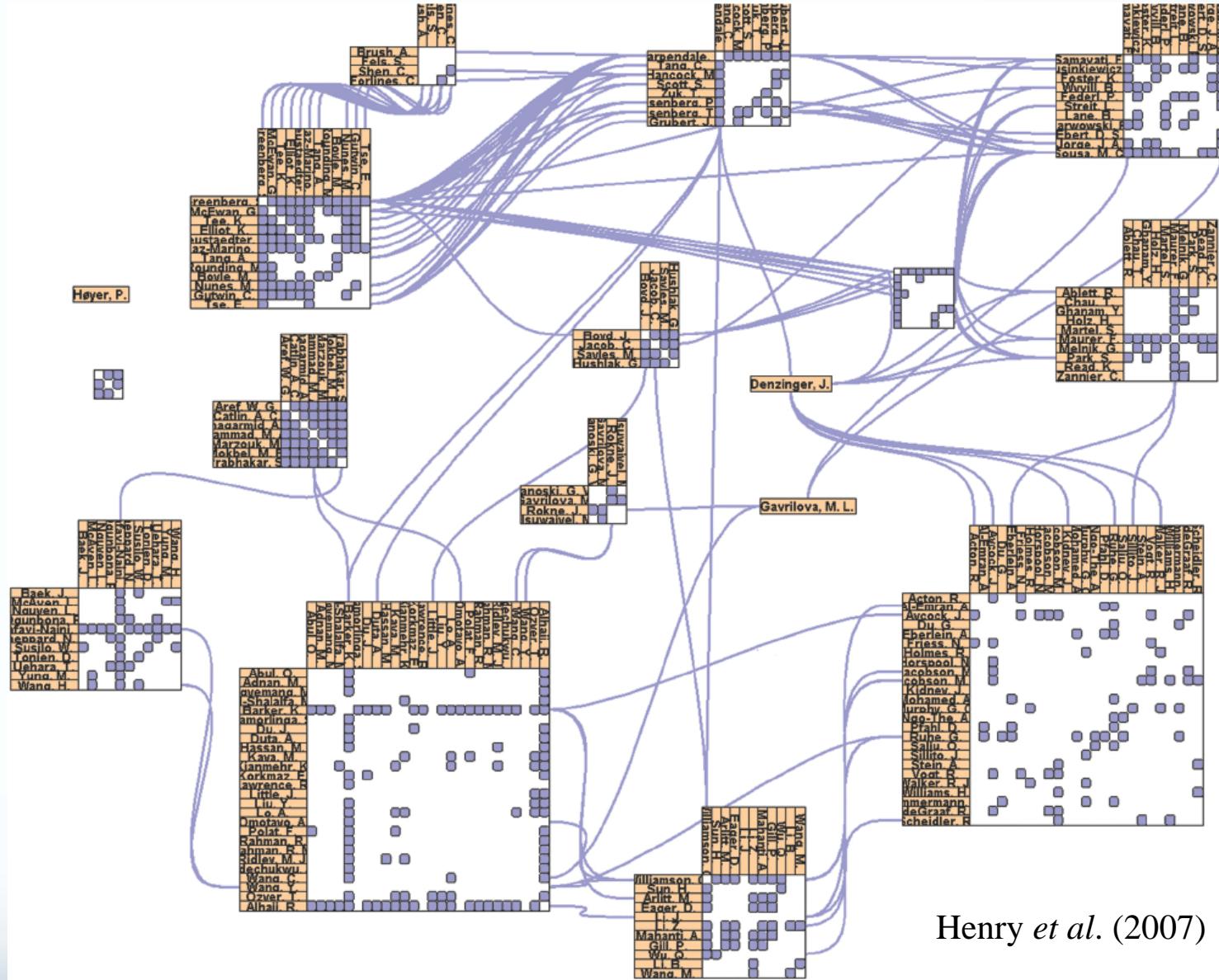
# Geovisual Analytics

## Linked Animal-Human Visual Analytics (LAHVA)



# Network Visualization

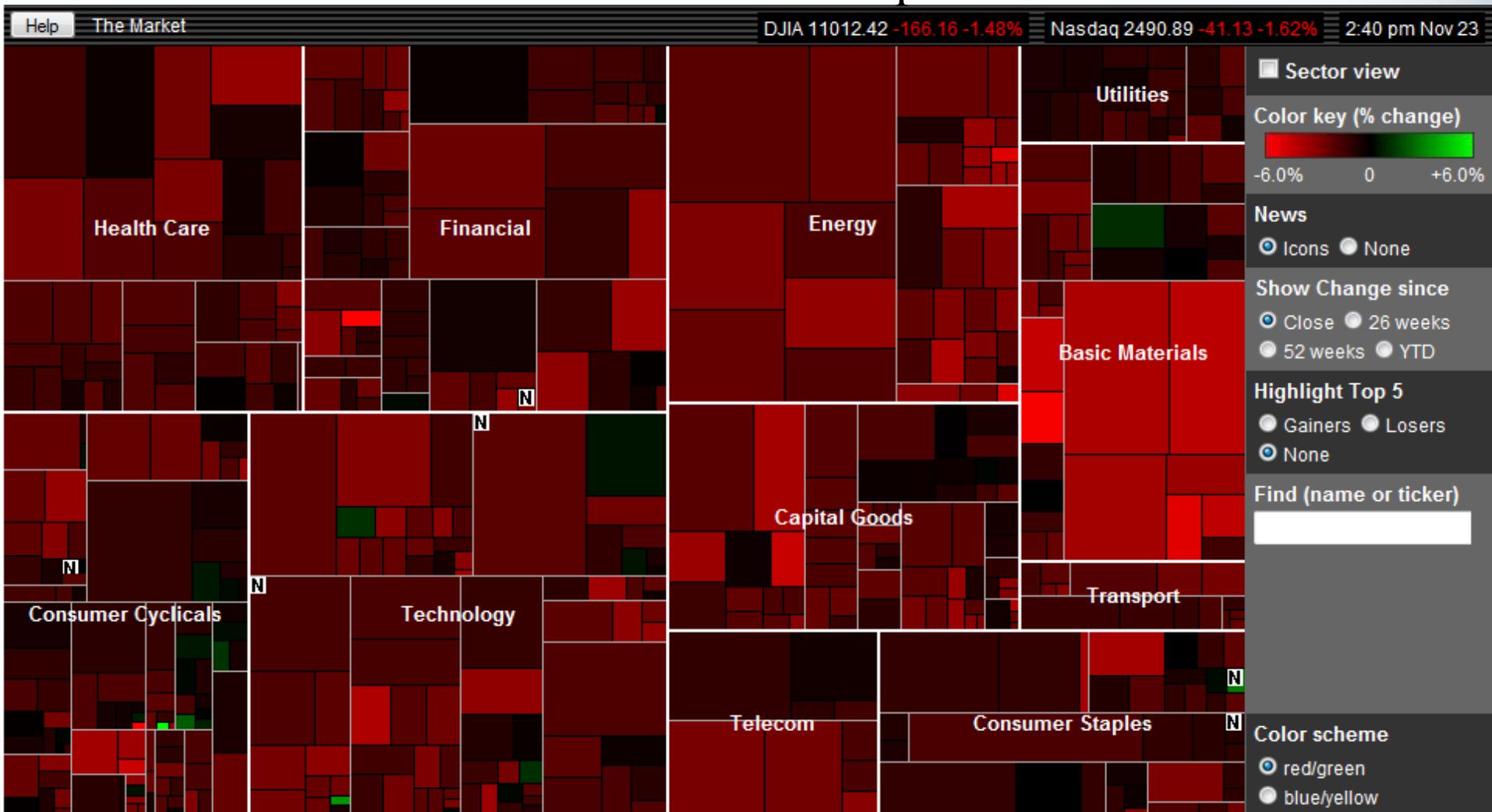
# NodeTrix Social Network Visualization



Henry *et al.* (2007)

# Hierachical Display

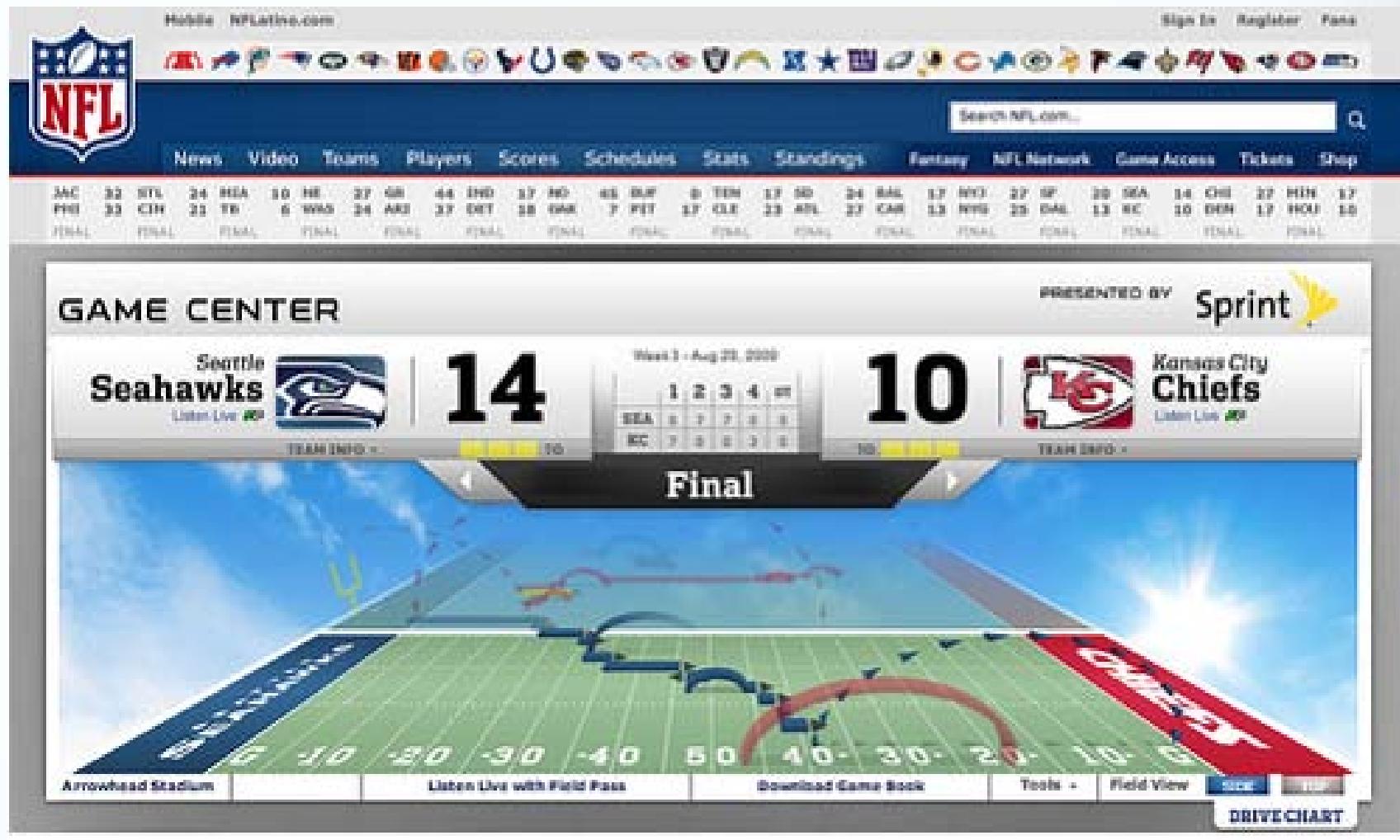
## Stocks Treemap



SmartMoney (2010)

# Temporal Visualization

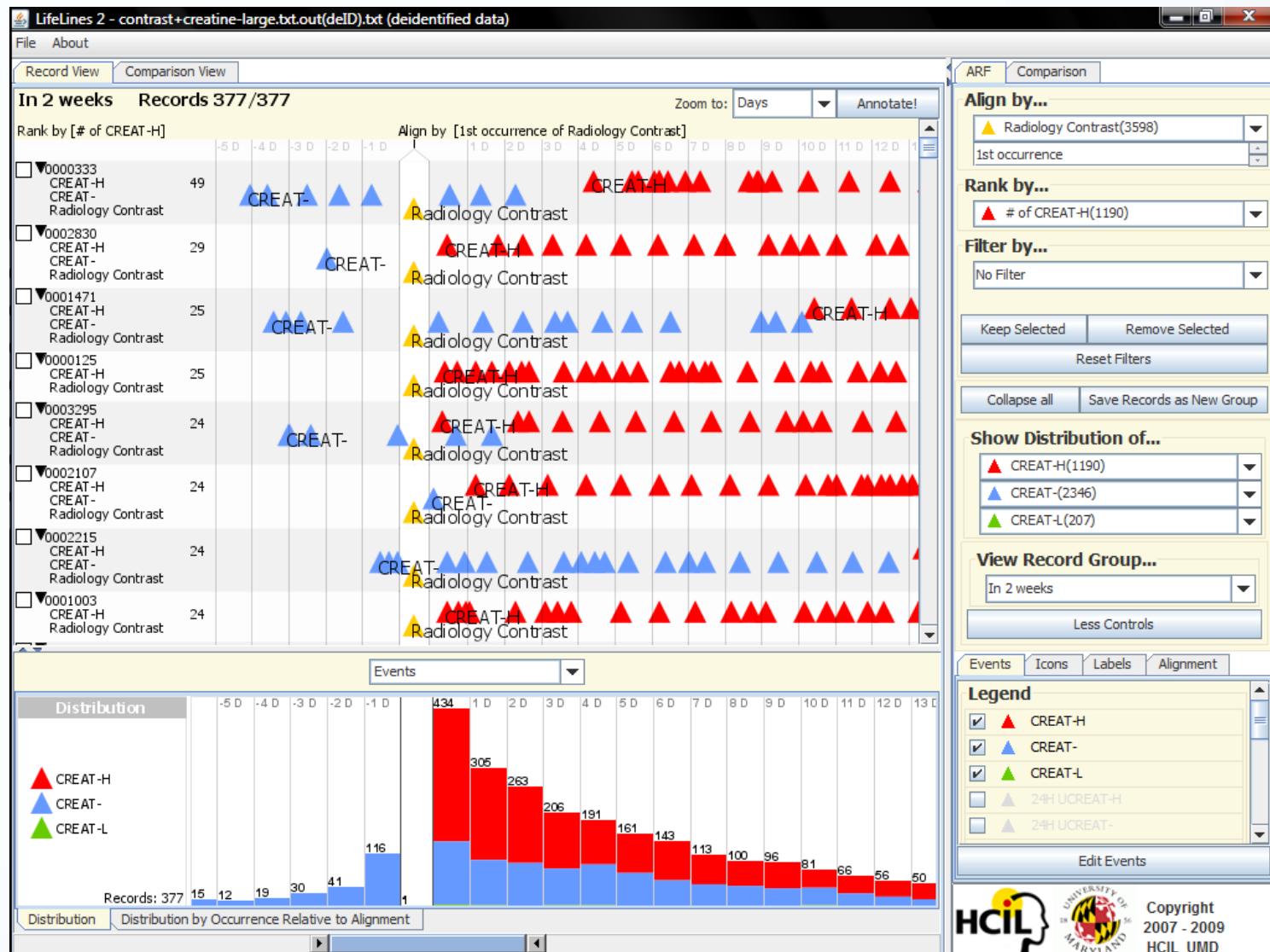
## NFL Drive Chart



Gunderson (2009)

# Temporal Analytics

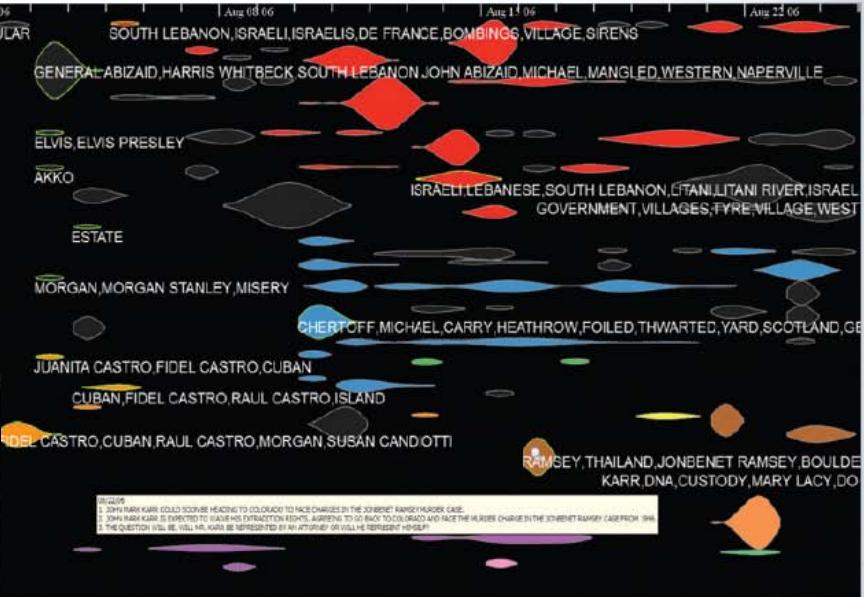
# Lifelines2



# Multimedia and Video Analytics

## New Streams Event River

Savvy



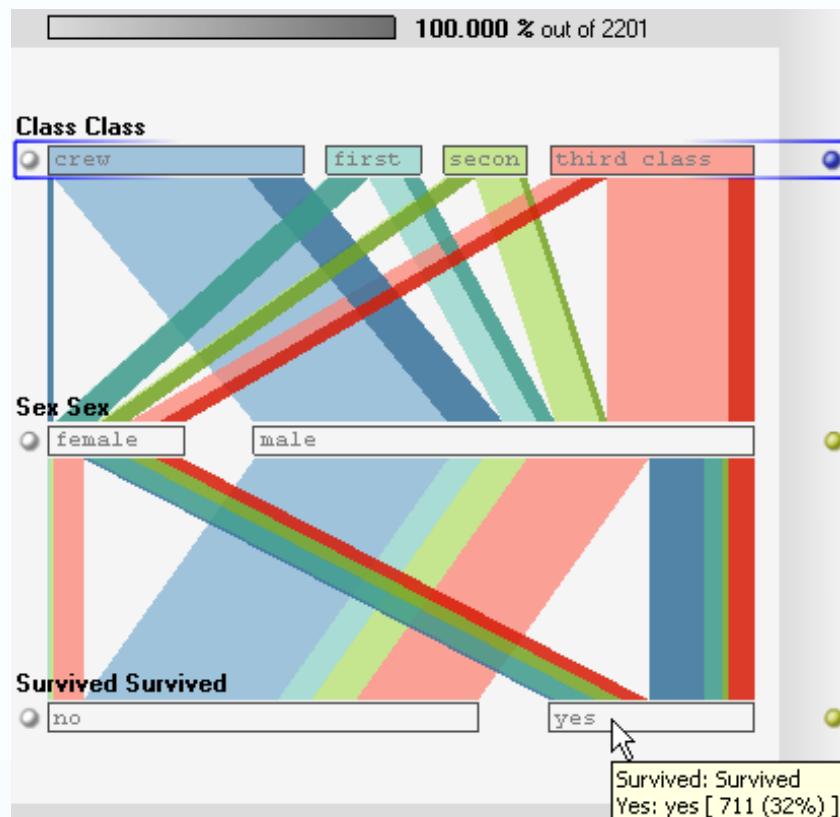
Ribarsky (2009)

Video Analytics tools  
are starting to emerge

Payne (2011)

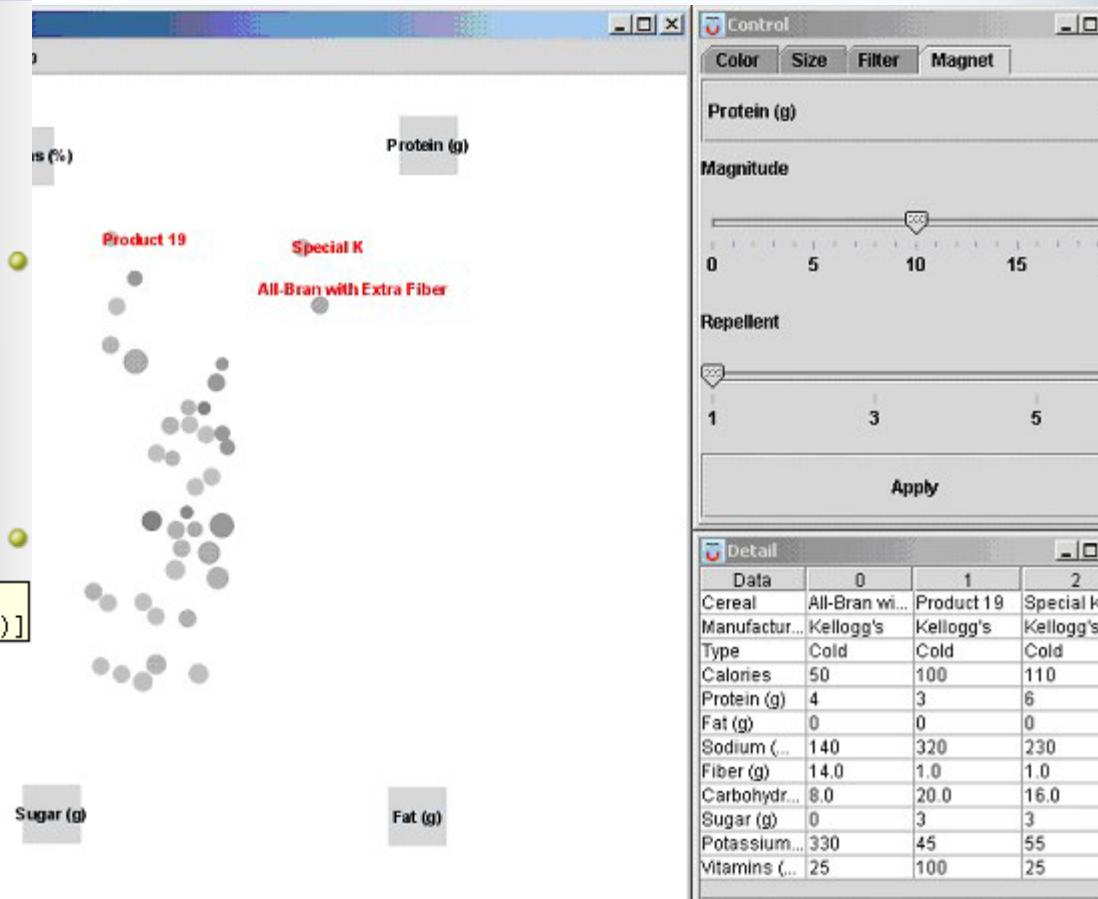
# Multivariate Analysis

## Parallel Sets



Bendix *et al.* (2005)

## Dust & Magnets

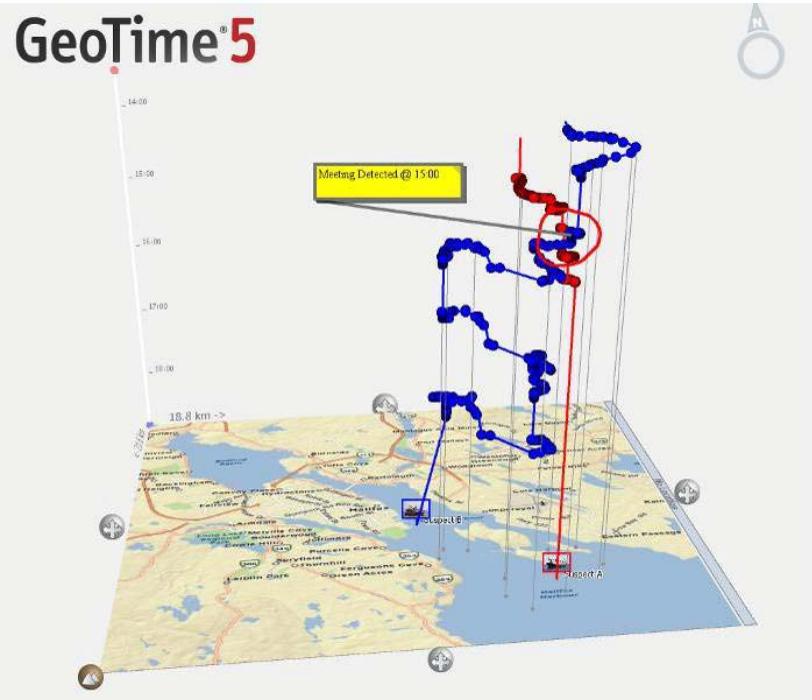


Soo Yi *et al.* (2005)

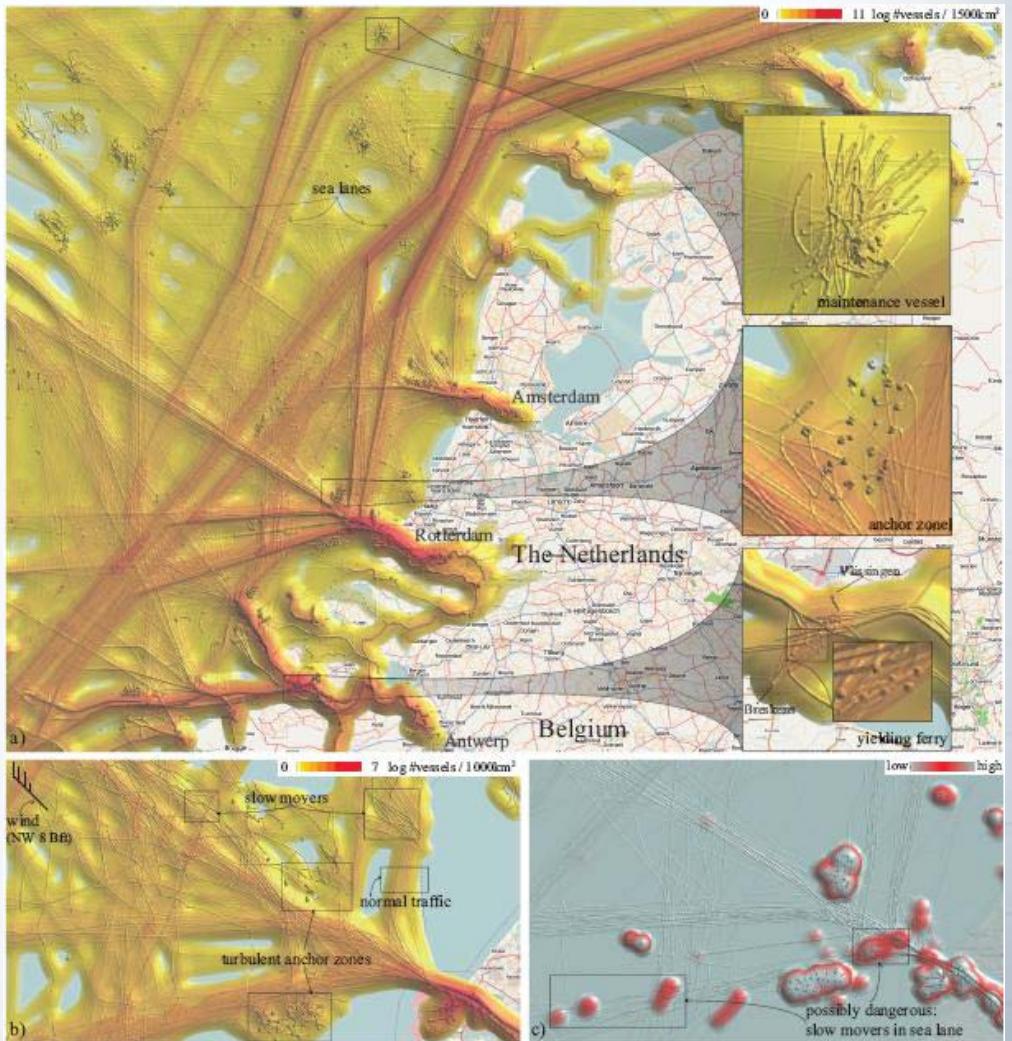
# Maritime Domain Awareness

## Shipping Density Landscapes

GeoTime<sup>®</sup>



Oculus Info Inc



Willems *et al.* (2009)

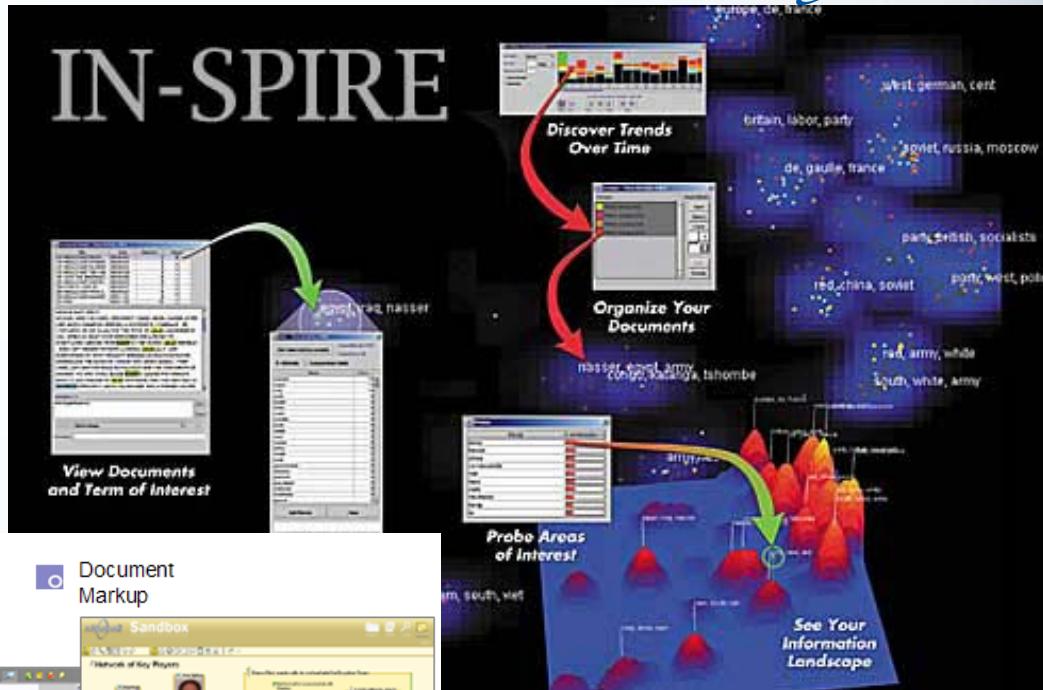
# Military Intelligence



nSpace



## System of Systems



PNNL (2011)

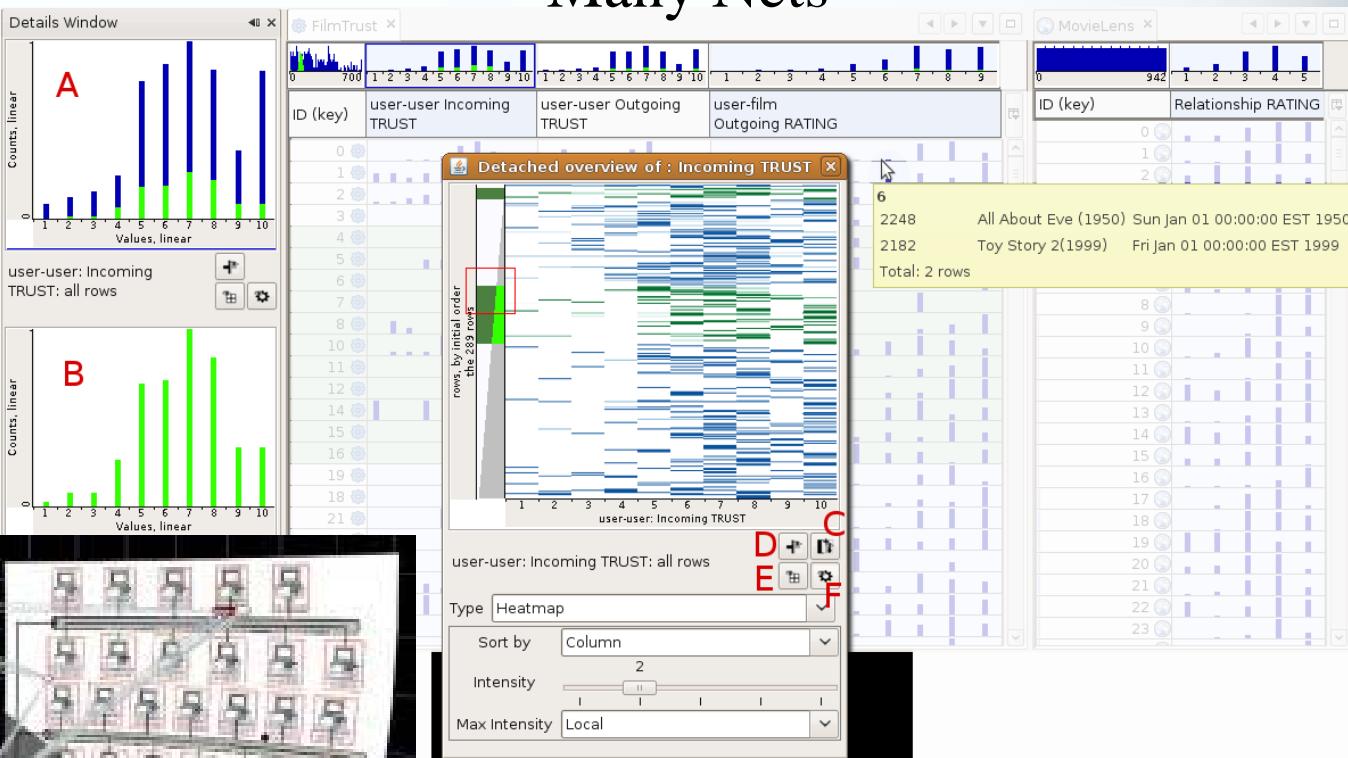
# Emergency Management

## Precision Information Environments



# Cyber Warfare

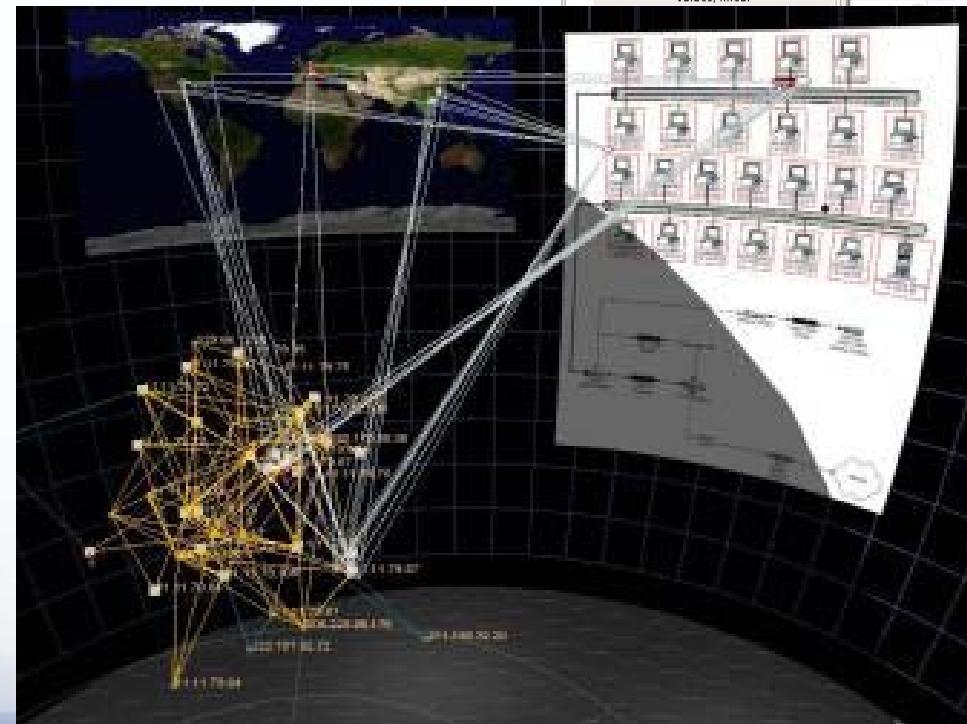
## Many Nets



Sopan *et al.* (2010)

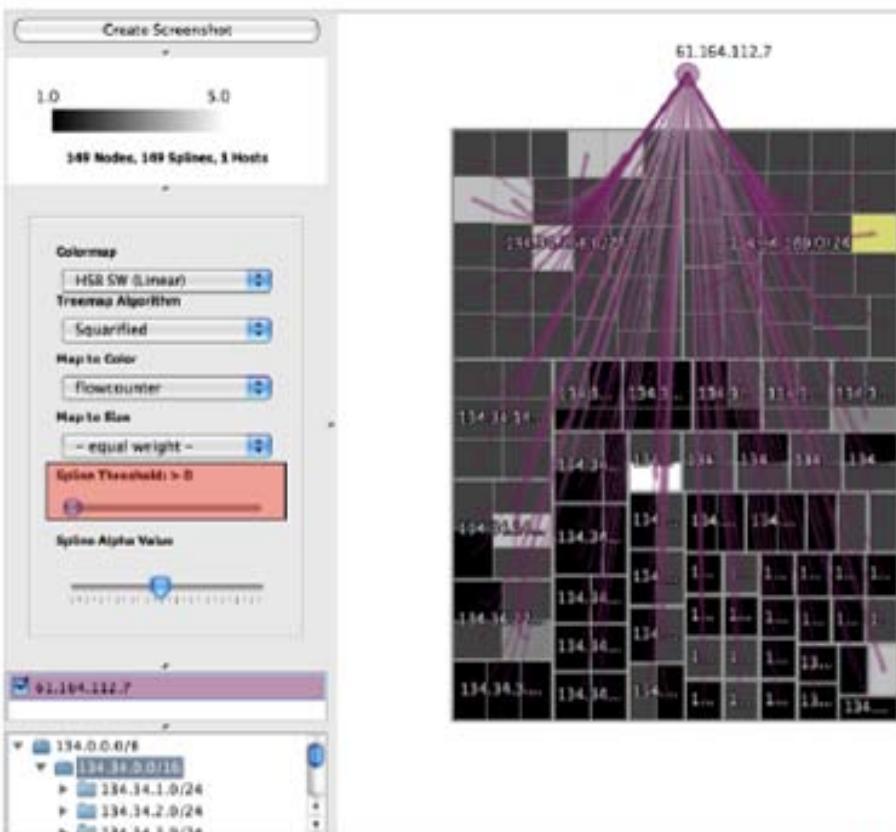
## Starlight Visual Information System

Future Point Systems (2011)

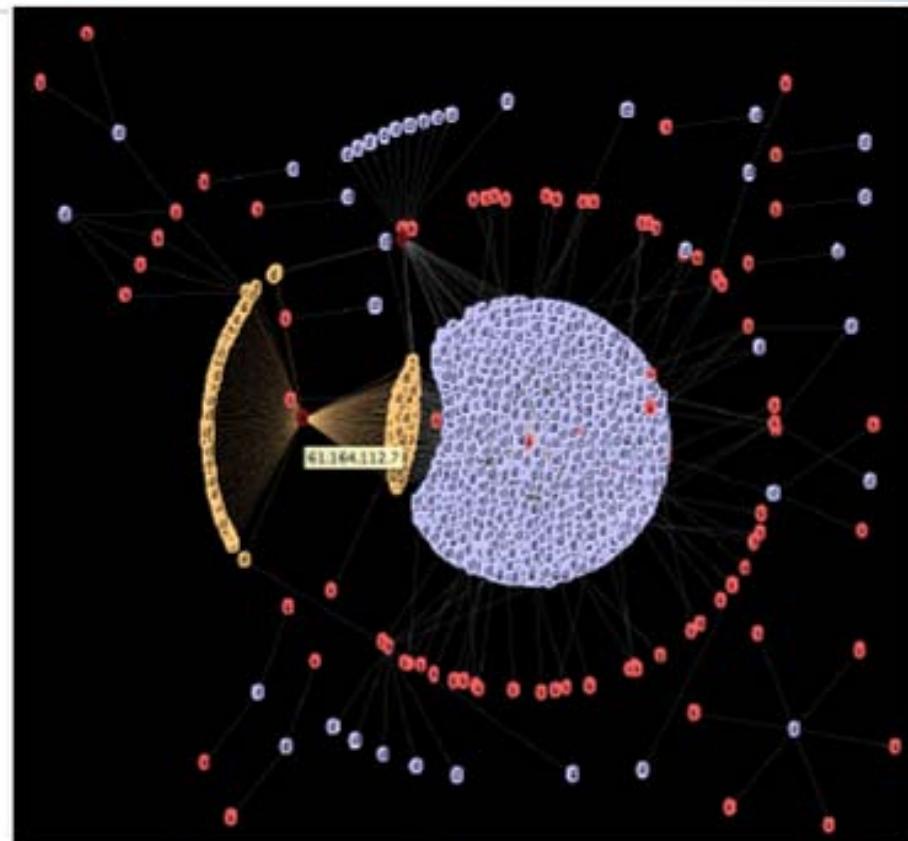


# Cyber Warfare

## NFlowVis



(a) Identification of compromised hosts using threshold adjustment (red).



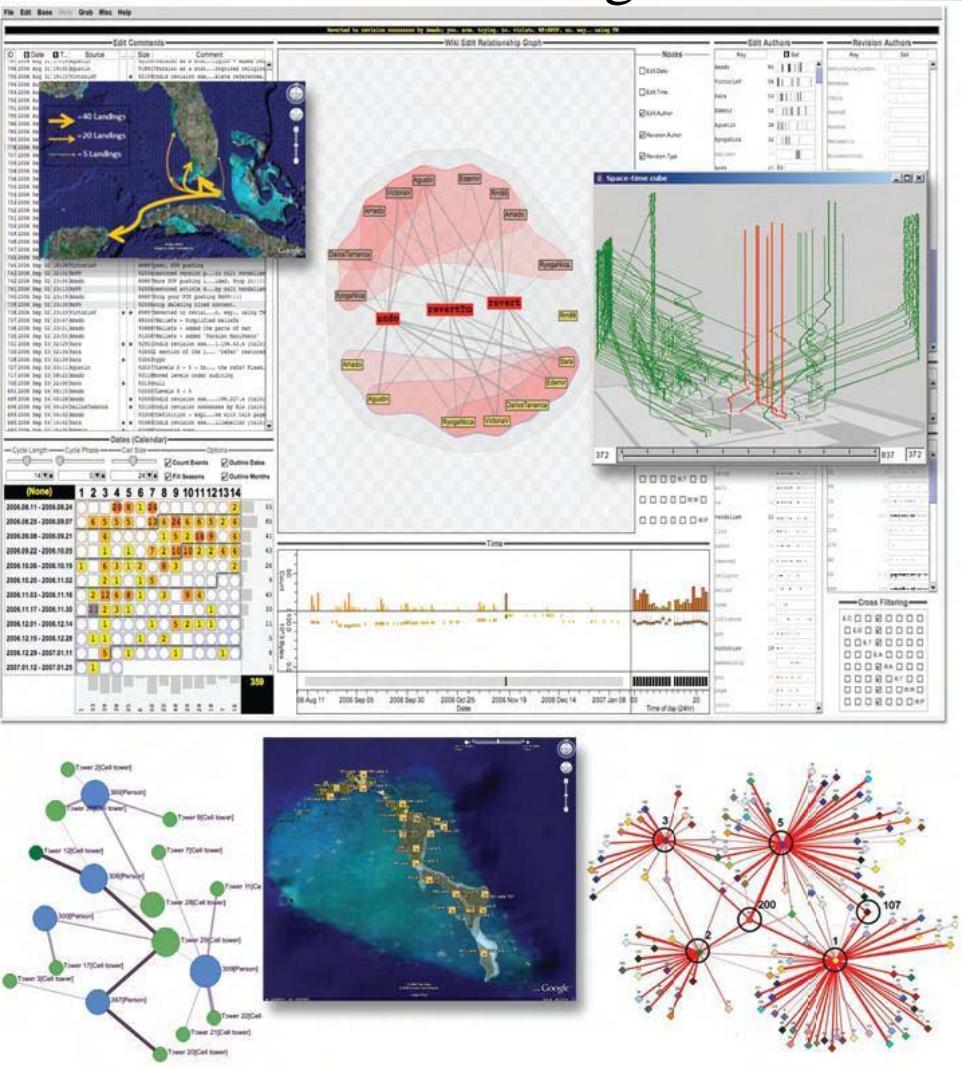
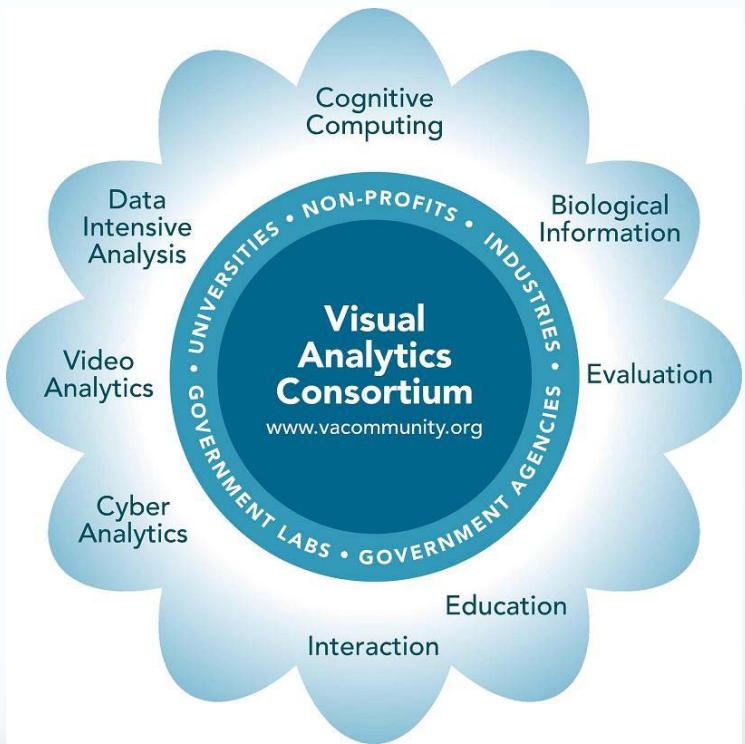
(b) Graph visualization showing communication flows between source (red) and destination hosts (blue).

Mansmann *et al.* (2009)

# Resources

# VAST Challenges

- VADL
- InfoVis:Wiki
- VAC Views
- ivac.org



VAST(2008)



[valerie.lavigne@drdc-rddc.gc.ca](mailto:valerie.lavigne@drdc-rddc.gc.ca)  
[denis.gouin@drdc-rddc.gc.ca](mailto:denis.gouin@drdc-rddc.gc.ca)